802.11g
Wireless Broadband Router

User Manual

Version 1.1

Copyright © 2003 by manufacturer. All rights reserved.

No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from the copyright owner.

All the other trademarks and registered trademarks are the property of their respective owners.

Statement of Conditions

The content described in this manual may be improved or changed at any time and it is subject to be changed without notice.

Manufacturer assumes no responsibility for errors contained herein or for direct, indirect, special, incidental or consequential damages with the furnishing, performance, or use of this manual or equipment supplied with it, even if manufacturer of its suppliers have been advised of the possibility of such damages.

Electronic Emission Notices

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device will accept any interference received, including interference that may cause undesired operation.

FCC Radio Frequency Interference Statement

This equipment has been tested and found to comply with the limits for a class B digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user need to correct the interference at his area. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

- Plug the equipment into an outlet that is on a different circuit from the television or radio.
- Change the direction of the television or radio antenna until the interference disappears.
- Move the equipment to one side or the other of the television or radio.
- Move the equipment farther away from the television or radio.

To assure continued compliance, any changes or modifications not expressly approved by manufacturer could void the user's authority to operate the equipment.

FCC Radiation Exposure Statement

This device and its antenna must operate with a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter. End users must be provided with specific operating instructions for satisfying RF exposure compliance.

Regulatory information / Disclaimers

Installation and use of this Wireless LAN device must be in strict accordance with the instructions included in the user documentation provided with the product. Any changes or modifications (including the antenna) made to this device that are not expressly approved by manufacturer may void the user's authority to operate the equipment. The manufacturer is not responsible for any radio or television interference caused by unauthorized modification of this device, or the substitution or attachment of connecting cables and equipment other than manufacturer specified. It is the responsibility of the user to correct any interference caused by such unauthorized modification, substitution or attachment. Manufacturer and its authorized resellers or distributors will assume no liability for any damage or violation of government regulations arising from failing to comply with these guidelines.

Table of Contents

1. Introduction 5
1.1 Features 5
2. Installation 8
2.1 Package Contents 8
2.2 Hardware Description 8
2.3 The Router's Front Panel 9
2.4 The Router's Rear Panel 10
2.5 System Requirement 10
2.6 Installation Procedure 10
2.7 Configuring Your Computers for Networking TCP/IP 11
3. Device Administration 20
3.1 Web Based Configuration 20
3.1.1 Device Information 21
3.1.2 Administration 21
3.1.3 Quickly Setup 24
3.1.4 Online Help 28
3.1.5 EZ Setup - WAN 29
3.1.6 EZ Setup - LAN 33
3.1.7 EZ Setup – Wireless (802.11g) 36
3.2 Telnet Configuration 43
4. Firewall and Advanced Functions 44
4.1 Access Control 44
4.2 MAC Filter 45
4.3 Service Time Allocation 46
4.4 LAN PC Management 48
4.5 URL Blocking 49
4.6 Virtual Server 49
4.7 DMZ 51
4.8 Multiple DMZ Host 52
4.9 Auto 2-Way Applications 53
4.10 Dynamic DNS 54
4.11 UPnP (Universal Plug and Play) 56
5. Troubleshooting 57
5.1 Common Problems & Solutions 57
5.2 Frequently Asked Questions 58

Appendix A Well-known TCP/IP Ports 61
Appendix B Illustrated Typical Application 62
Appendix C Cabling and Pin Assignment 64
Appendix D Configure IP manually 66
Appendix E Technical Information 68

1. Introduction

Congratulations on your purchase of this outstanding 802.11g Wireless Broadband Router. This product is a perfect option to connect a group of wired or wireless PCs to a high-speed Broadband Internet connection or to an Ethernet based Backbone (ETTH/ETTB: Ethernet To The Home/Building). Configurable as a DHCP server, this product is the only externally recognized server device on your local area network (LAN). Thus even a non-technical person can easily configure it to meet the versatile applications.

This product does not only provide a complete solution to share the Internet bandwidth, it also serves as an Internet Firewall to protect your LAN data from being accessed by outside intruders/hackers (Refer to Figure 1.1). Since all incoming data packets have been inspected/analyzed, all unwanted packets may be filtered-out and be recorded as an intrusion event. The router can also be configured to block some internal LAN user's access to the Internet for management purpose.

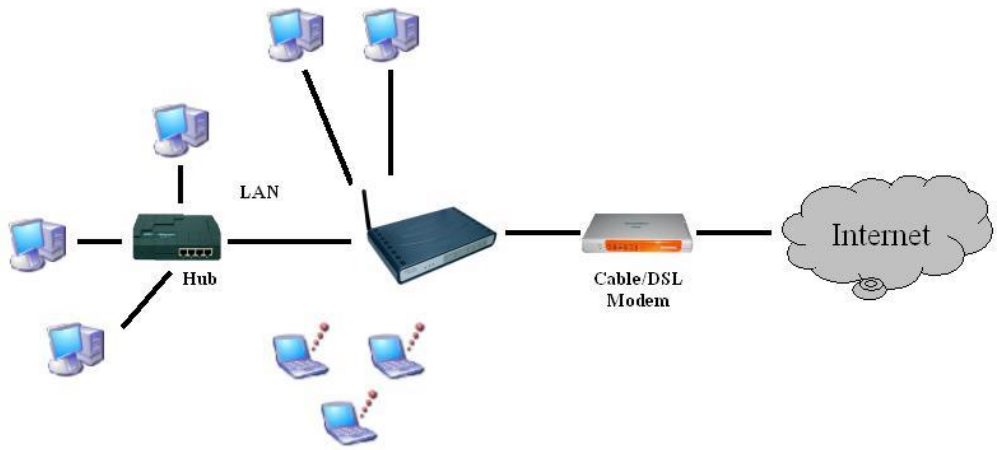


Figure 1.1 Secure Internet Access via Cable/DSL Modem

1.1 Features

- Local Area Network (LAN) connection via 10/100Mbps Ethernet ports or 54Mbps wireless interface (up to 253 users, including up to 64 wireless users).
- Internet connection (WAN) to cable/DSL modem or Ethernet backbone via a 10/100Mbps WAN port.
- Fully compatible with IEEE 802.11g wireless LAN standard and interoperable with any 802.11g or 11b compliant equipments.
- Wireless interface supports 64/128-bit WEP (Wired Equivalent Privacy) encryption,

802.1x, SSID broadcast disabled and MAC address filtering features.

- Integrated wireless AP (Access Point) and broadband router in one unit.
- Multiple WAN connection types:

  Static IP : for xDSL lease line or router-to-router interconnect.
  DHCP client : for most cable modem service.
  PPPoE : for Dial-up ADSL service.
  PPTP client : for some specific Dial-up ADSL or Layer2-VPN application.
- Equipped with a 4-port 10/100Mbps switch (with auto crossover) for LAN users.
- DHCP Server/ DNS proxy support.

  All the networked computers in LAN can retrieve TCP/IP setting (IP address, subnet mask, gateway, DNS…) automatically from this device.
- Simultaneously acts as both DHCP Server on the LAN and a DHCP Client on the WAN for most easy application.
- Connects multiple LAN PCs to the Internet with only one dynamic-assigned IP address (NAT mode) or a range of legal IP address (NAT/Routing mode).
- Web-based Configuration.
- Allow/Deny remote administration through WAN connection by Web browser.
- Supports Telnet/Console administration from a networked computer in LAN.
- Firewall capability to protect LAN PCs from outside intruder accesses/attacks.

  Avoid unwanted packets from WAN and provide a system event log to record intrusion information (Date/time, source IP address & port…).
- LAN user Access right

  Administrator can arrange interior LAN user's access right to Internet by MAC address, IP address, TCP/IP port number, URL keywords and a pre-defined time table.
- Virtual Server (Port forwarding) function

  Internet servers (WWW, FTP, E-mail…) in LAN could be virtually exposed to WAN for outside Internet user. This is a useful and secure network deployment for Internet servers.
- DMZ (De-Militarized Zone) Host

  Administrator can totally expose a host PC in LAN to the Internet without any firewall protection mechanism. This option allows a full two-way communication between the local host PC and remote Internet node. (ex. bi-directional games, video/audio conferences…)
- Multi DMZ Host support

  In static IP configuration with a range of legal IP address, administrator could totally expose more host PCs in LAN to the Internet according to LAN/WAN IP address mapping.

- Auto 2-way Applications

  Provides an automatic mechanism to support some specific applications, which need one or many incoming ports when they connect with application servers in Internet. (Like Microsoft Game Zone, Battle.net…)

- Dynamic DNS

  Via www.dyndns.org DNS service provider, your registered domain name could be updated automatically whenever system's WAN IP is changed.

- UPnP (Universal Plug and Play) supported

2. Installation

2.1 Package Contents

The product package should contain the following items:

- Cable/DSL wireless broadband router
- CD-ROM (User manual)
- Power adapter

If any of the parts are incorrect, missing, or damaged, please contact your vendor. Retain the carton and the original packing materials in case you need to return the product.

2.2 Hardware Description

The router can be connected to the Internet or to a remote site using its RJ-45 WAN port. It can be connected directly to your PC to a local area network using any of the Fast Ethernet LAN ports.

Access speed to the Internet depends on your service type. However, data passing between devices connected to your local area network can run up to 100 Mbps over the Fast Ethernet ports.

The router includes an LED display on the front panel for system power and port indications that simplifies installation and network troubleshooting. It also provides four RJ-45 LAN ports and one RJ-45 WAN port on the rear panel.

- 4 RJ-45 ports for connection to a 10BASE-T/100BASE-TX Ethernet Local Area Network (LAN). These ports can auto-negotiate the operating speed to 10/100 Mbps, the mode to half/full duplex, and the pin signals to MDI/MDI-X (i.e., allowing these ports to be connected to any network device with straight-through cable). These ports can be connected directly to a PC or to a server equipped with an Ethernet network interface card, or to a networking device such as an Ethernet hub or switch.

- One RJ-45 port for connection to a DSL or cable modem (WAN). This port also auto-negotiates operating speed to 10/100 Mbps, the mode to half/full duplex, and the pin signals to MDI/MDI-X.

2.3 The Router's Front Panel

The front panel contains the status LEDs described below:

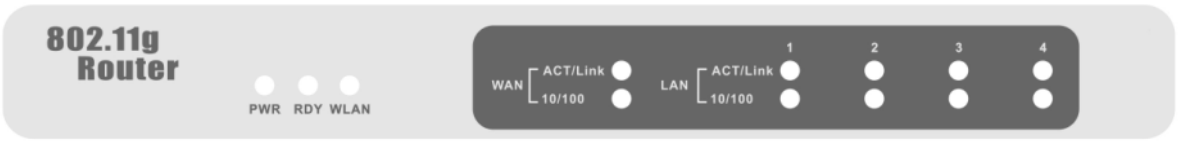


Figure 2.1 Front Panel

Device Indicators

LED	Status	Description
PWR	On	Power is supplied to the router.
	Off	Power is not supplied to the router.
RDY	Blinking once per second	The router is working normally.
	Blinking faster or be off	Something wrong with the router.
WLAN	On	The wireless interface is ready for services.
	Off	The wireless interface fails or is turned off.
	Blinking	Wireless port is transmitting or receiving data.

WAN Indicators

LED	Status	Description
ACT/Link	On	The WAN port has detected a valid network connection.
	Blinking	The WAN port is transmitting or receiving data.
10/100	On	Indicates 100Mbps network connection.
	Off	Indicates 10Mbps network connection.

LAN Indicators

LED	Status	Description
ACT/Link	On	The indicated LAN port has detected a valid network connection.
	Blinking	The indicated LAN port is transmitting or receiving data.
10/100	On	Indicates 100Mbps network connection.
	Off	Indicates 10Mbps network connection.

2.4 The Router's Rear Panel

The rear panel contains the port connections described below:

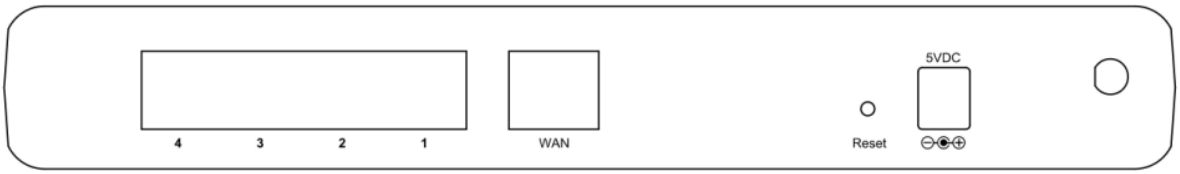


Figure 2.2 Rear Panel

Items	Description
Power Inlet	Connect the included power adapter to this inlet. **Warning**: Using the wrong type of power adapter may damage your router.
Reset Button	Use this button to restore the default factory settings.
WAN Port	Connect your cable/DSL modem, or an Ethernet router to this port.
LAN Ports	Connect devices (such as a PC, hub or switch) on your local area network to these ports.
Wireless antenna	Rotate antenna to the best position for more effective coverage.

2.5 System Requirement

- One Ethernet based broadband Internet connection (like cable/ADSL modem or others)
- One PC with a NIC card or 802.11b/g adaptor, and installed TCP/IP protocol stack.
- Microsoft Internet Explorer 5 or later (Netscape V6/7 or later) web browser.
- TCP/IP network protocol installed on each PC that needs to access the Internet.

2.6 Installation Procedure

- Connect the Power Adapter

  Plug the power adapter into the power inlet on the router, and the other end into a power outlet. Check the **Power** LED on the front panel to make sure it is on.

- Connect the WAN

  Use twisted-pair cable to connect the Cable/DSL modem to the WAN port on the rear of the router. Check if the **ACT/Link** LED is on. (Please refer to Appendix C for detailed cabling and pin assignment).

- Connect the LAN

  Use twisted-pair cable to connect one of the LAN ports on the router to your computer's network adapter. Or, cascade any of the LAN ports on the router to an Ethernet hub or switch, and then connect your PC or other network device to the hub or switch.

  If it is correctly connected, the responding **ACT/Link** LED will be on.

  You may also connect the router to your PC (using a wireless client adapter) via radio signals.

Note:

Since all the WAN and LAN ports have auto crossover capability, you could use a flat RJ-45 cable or a crossover cable as you wish.

Once both WAN and LAN are connected successfully, please hold down the reset button continuously for 5 seconds to make sure the router is under factory default condition now.

2.7 Configuring Your Computers for Networking TCP/IP

To access the Internet through the router, you have to configure the network settings of the computers on your LAN correctly to use the same IP subnet as the router. The default network settings for the router are:

Gateway IP Address: 192.168.8.1
Subnet Mask: 255.255.255.0

The IP address of the connected client PC should be 192.168.8.x (where x means 2 ~ 254). You can set the IP address for client PCs either by automatically obtaining an IP address from the router's DHCP server or by manual configuration.

Note:

1. The router is shipped pre-configured as a DHCP server (offers IP range from 192.168.8.**17** through 192.168.8.**128** by default). It automatically assigns the following TCP/IP configuration information when the PCs are rebooted:
   - IP address — 192.168.8.17 ~ 192.168.8.128
   - Subnet mask — 255.255.255.0
   - Gateway address — 192.168.8.1
2. These settings may be changed to suit your network requirements, but you must first configure at least one computer to access the router's web configuration interface.

Configuring Your Computer in Windows 9x/Me

Follow the steps below to set your computer as a DHCP Client. (If the fixed IP mode for administrator's computer is desired, please refer to Appendix D.)

1. On the Windows taskbar, click **Start/Settings/Control Panel**.
2. Double-click the **Network** icon.
3. Click the **Configuration** tab.
4. Double-click **TCP/IP** for your network card/adapter (See Figure 2.3).

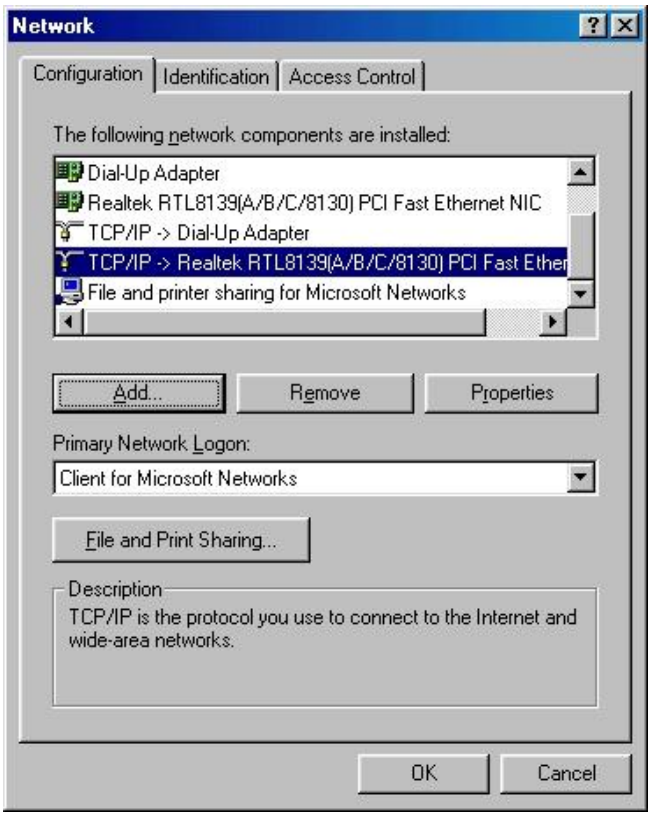


Figure 2.3 Select TCP/IP Protocol Option

5. On the **TCP/IP Properties** Window, click the **IP Address** tab. Enable the **Obtain an IP address automatically** option (See Figure 2.4).

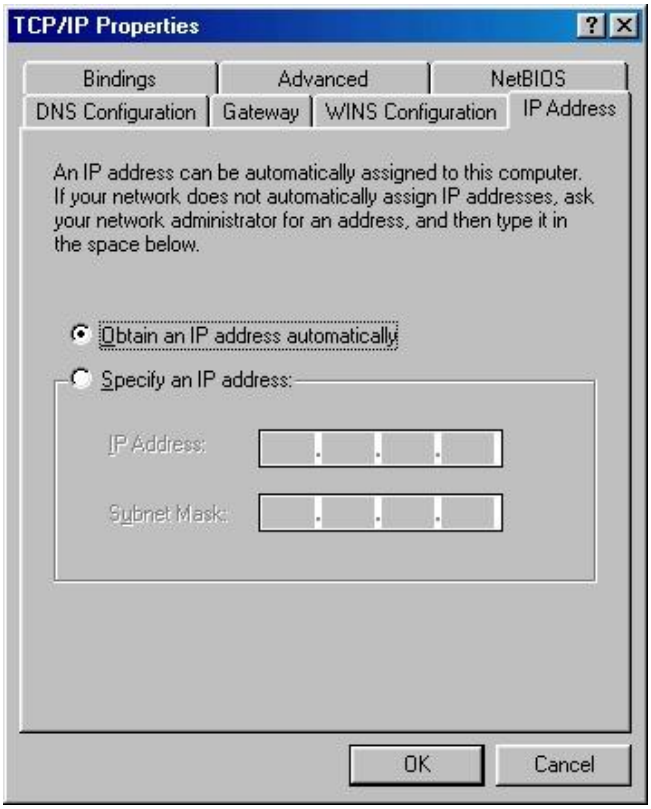

TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address automatically
Specify an IP address:
IP Address:
Subnet Mask:
OK
Cancel

Figure 2.4 Obtain IP Address

6. Click the **OK** button to close the **TCP/IP Properties** window.
7. On the Network window, click the **OK** button to save these settings.
8. Restart your PC.

Configuring Your Computer in Windows XP

Follow the steps below to set your computer as a DHCP Client. (If the fixed IP mode for administrator's computer is desired, please refer to Appendix D.)

1. On the Windows taskbar, click **Start/Settings/Control Panel**.
2. Double-click the **Network Connections** icon.
3. Double-Click the **Local Area Connection** icon.
4. Click the **Properties** button (See Figure 2.5).

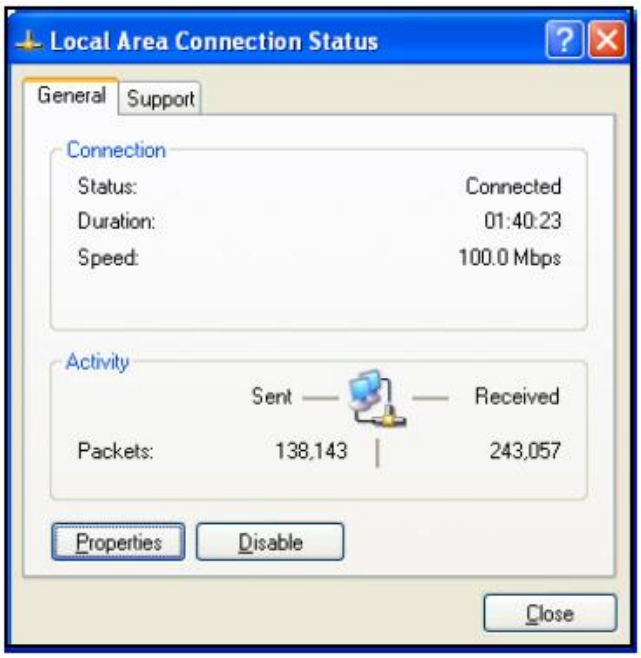


Figure 2.5 Local Area Connection

5. In the **Local Area Connection Properties** box, verify the box next to **Internet Protocol (TCP/IP)** is checked. Then highlight the **Internet Protocol (TCP/IP)**, and click the **Properties** button (See Figure 2.6).

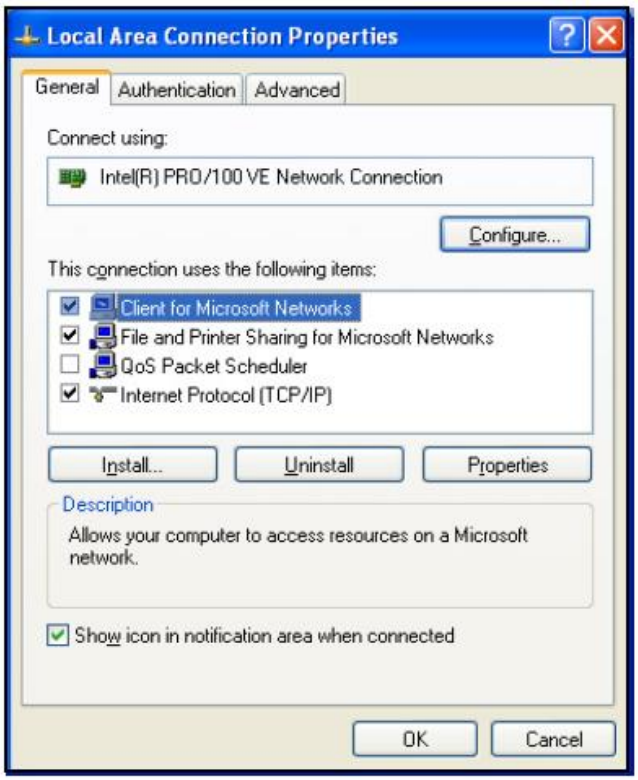


Figure 2.6 Local Area Connection Properties

6. Select **Obtain an IP address automatically** (Figure 2.7).
7. Select **Obtain DNS server address automatically**.

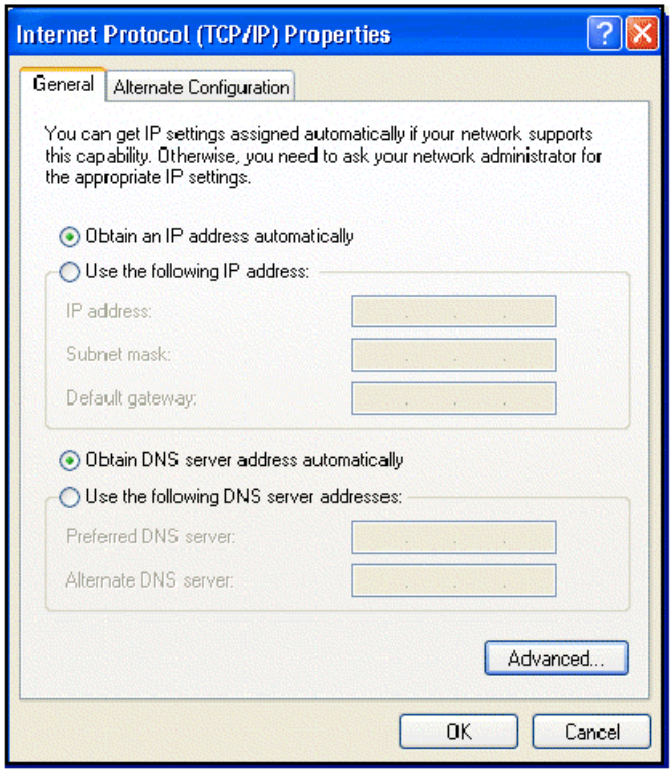

Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

Figure 2.7 Internet Protocol (TCP/IP) Properties

8. Click the **OK** button to save these settings.
9. Restart your PC.

Configuring Your Computer in Windows 2000

Follow the steps below to set your computer as a DHCP Client. (If the fixed IP mode for administrator's computer is desired, please refer to Appendix D.)

1. On the Windows taskbar, click **Start/Settings/Control Panel**.
2. Double-click the **Network and Dial-up Connections** icon.
3. Double-Click the **Local Area Connection** icon. When the Status dialog box window opens, click the **Properties** button.
4. In the **Local Area Connection Properties** box, verify the box next to **Internet Protocol (TCP/IP)** is checked. Then highlight the **Internet Protocol (TCP/IP)**, and click the **Properties** button (See Figure 2.8).
5. Select **Obtain an IP address automatically** (Figure 2.9).
6. Select **Obtain DNS server address automatically**.

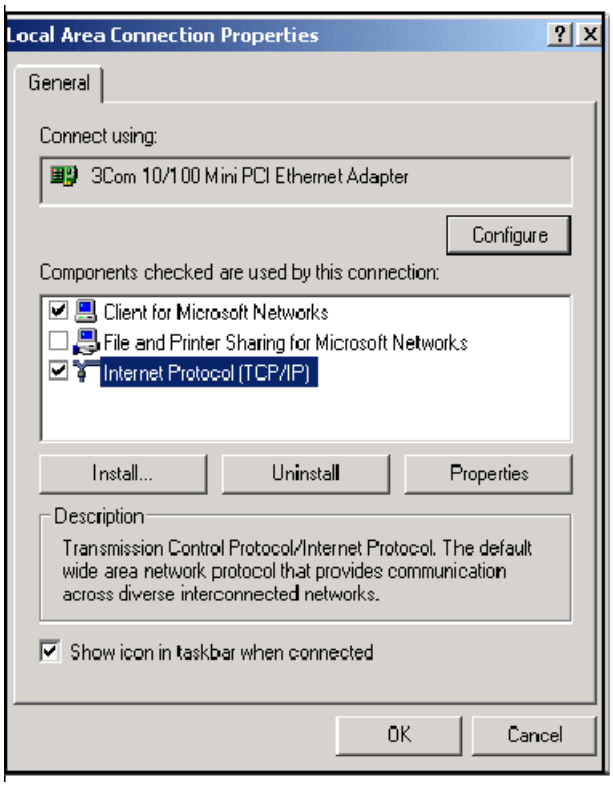


Figure 2.8 Local Area Connection Properties

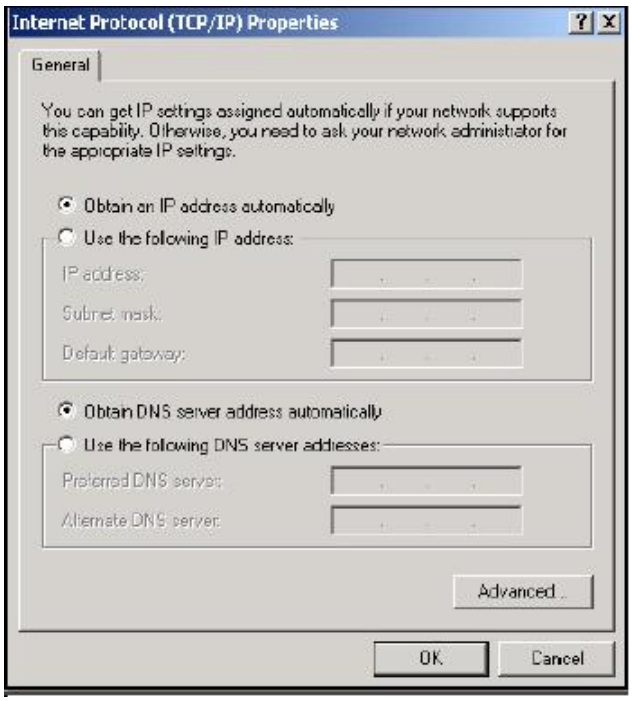

Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

Figure 2.9 Internet Protocol (TCP/IP) Properties

7. Click the **OK** button to save these settings and restart your PC.

Configuring Your Computer in Windows NT4

Follow the steps below to set your computer as a DHCP Client. (If the fixed IP mode for administrator's computer is desired, please refer to Appendix D.)

1. On the Windows taskbar, click **Start/Settings/Control Panel**.
2. Double-click the **Network** icon.

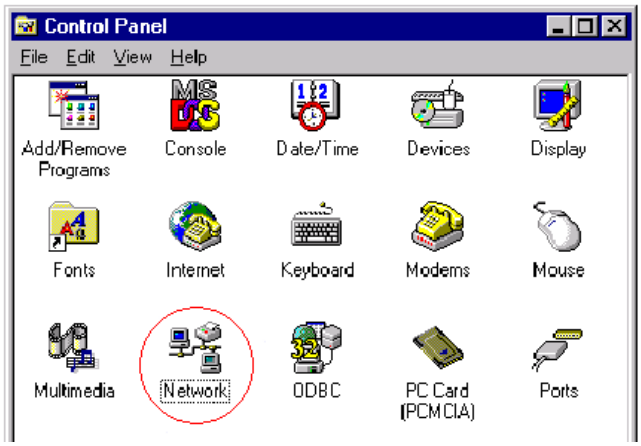


Figure 2.10 Control Panel – Network

3. Select the **Protocol** tab.
4. Double-click **TCP/IP Protocol** (See Figure 2.11).

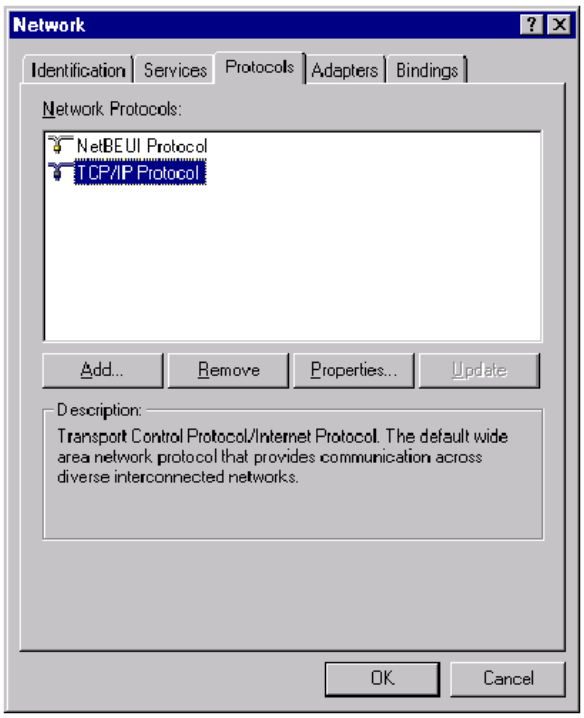


Figure 2.11 TCP/IP Protocol

5. Select the **IP Address** tab (Figure 2.12).
6. Select **Obtain an IP address from a DHCP server**.

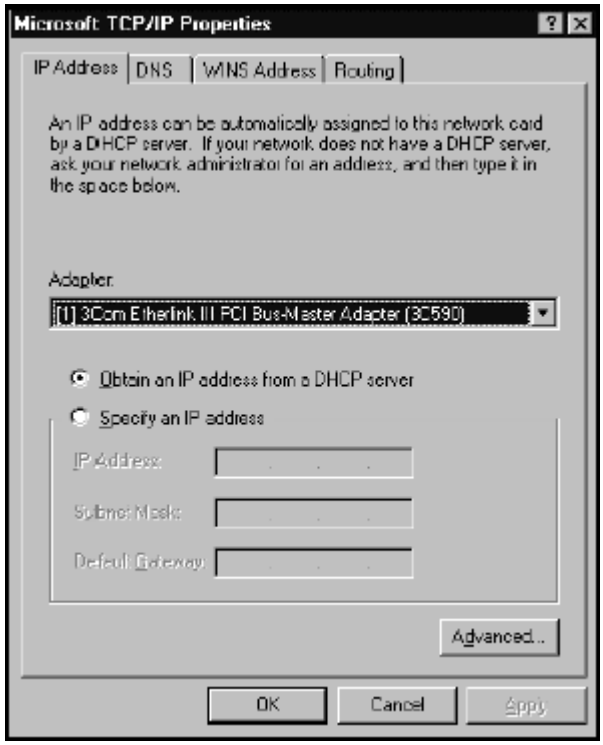

Microsoft TCP/IP Properties
IP Address
DNS
WINS Address
Routing
An IP address can be automatically assigned to this network card by a DHCP server. If your network does not have a DHCP server, ask your network administrator for an address, and then type it in the space below.
Adapter:
[1] 3Com EtherLink III PCI Bus-Master Adapter (3C590)
Obtain an IP address from a DHCP server
Specify an IP address
IP Address:
Subnet Mask:
Default Gateway:
Advanced...
OK
Cancel
Apply

Figure 2.12 TCP/IP Properties

7. Click the **OK** button to save these settings.
8. Restart your PC.

Verifying TCP/IP Properties:

Windows 9x/Me:

1. On the Windows taskbar, click **Start/Run**.
2. Type **winipcfg**, and then click the **OK** button (See Figure 2.13).

Figure 2.13 Check Screen under Windows 9x/Me

3. The IP configuration window opens. (See Figure 2.14)
4. Verify that your IP Address is 192.168.8.x, Subnet Mask is 255.255.255.0 and Default Gateway is 192.168.8.1.

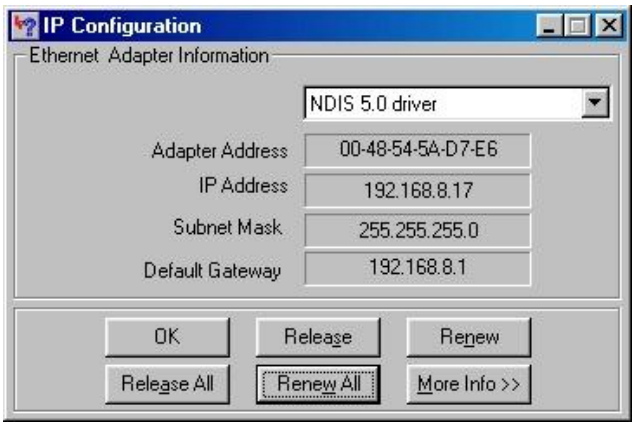


Figure 2.14 Ethernet Adapter Information

Windows XP/2000/NT4:

1. On the Windows taskbar, click **Start/Program/Command Prompt**.
2. Type **ipconfig /all** and press the <Enter> key. Verify that your IP Address is 192.168.8.x, Subnet Mask is 255.255.255.0 and Default Gateway is 192.168.8.1 (See Figure 2.15).

```
C:\>ipconfig /all

Windows 2000 IP Configuration

        Host Name . . . . . . . . . . . . : sw
        Primary DNS Suffix  . . . . . . . : eglx.com.tw
        Node Type . . . . . . . . . . . . : Hybrid
        IP Routing Enabled. . . . . . . . : Yes
        WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Local Area Connection 2:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : Realtek RTL8139(A) PCI Fast Ethernet
 Adapter #2
        Physical Address. . . . . . . . . : 00-48-54-5A-D7-E6
        DHCP Enabled. . . . . . . . . . . : No
        IP Address. . . . . . . . . . . . : 192.168.8.1
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . :
        DNS Servers . . . . . . . . . . . :
```

Figure 2.15 Check Screen under Windows XP/2000/NT4

In case there is something wrong, please refer to Section 5 for troubleshooting.

3. Device Administration

The router can be configured via Web browser/Telnet. Administrator can choose either one of the methods to perform device administration. No matter which method is used, this administration allows **only one login session at a moment**. This is due to the consideration of system database consistency. If there is any other one that intends to login simultaneously, none could succeed to login at that time and an alert message will pop-up.

The following description also assumes the router is under the factory default condition, and the WAN port is well connected.

3.1 Web Based Configuration

Open the web browser and enter http://192.168.8.1 in the browser's address box. This IP address is the router's LAN interface address.

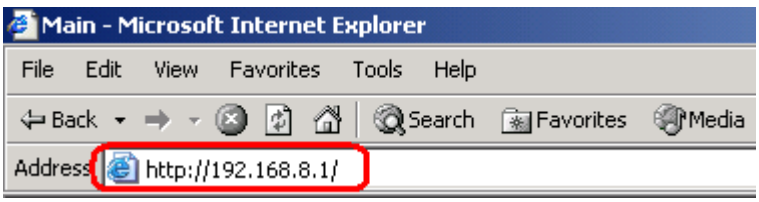

Main - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.8.1/

Figure 3.1 Open Web Browser and enter the router's default address

The home page displays the Device Status (Figure 3.2.).

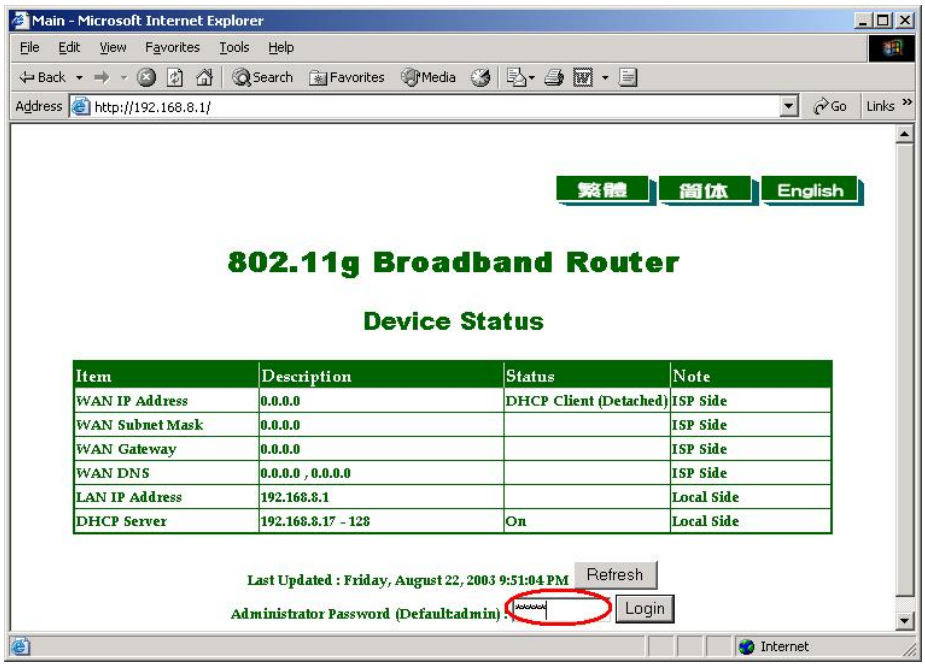

Main - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://192.168.8.1/
繁體 簡体 English
802.11g Broadband Router
Device Status
Item | Description | Status | Note
WAN IP Address | 0.0.0.0 | DHCP Client (Detached) | ISP Side
WAN Subnet Mask | 0.0.0.0 | | ISP Side
WAN Gateway | 0.0.0.0 | | ISP Side
WAN DNS | 0.0.0.0 , 0.0.0.0 | | ISP Side
LAN IP Address | 192.168.8.1 | | Local Side
DHCP Server | 192.168.8.17 - 128 | On | Local Side
Last Updated : Friday, August 22, 2003 9:51:04 PM
Refresh
Administrator Password (Default:admin)
Login
Internet

Figure 3.2 Home Page of The Router

Note:

This page is not protected by any password. It is used to provide all LAN users to inquire the router's device status at any time.

Enter the default Administrator Password **admin** and click **Login**.

3.1.1 Device Information

After login, the first page shown is the **Device Information** of the router (See Figure 3.3).
In this page, it shows the detailed status of the router and displays the current WAN's information about dial-up duration and traffic (bytes count).

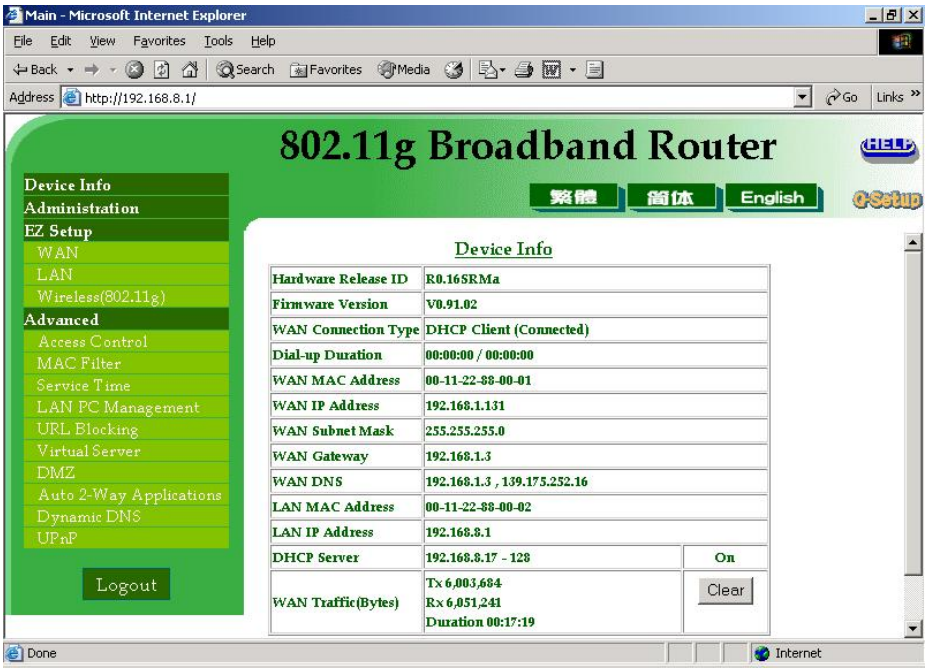


Figure 3.3 Device Information of The Router

You can click the **Clear** button to clear the WAN traffic counter, and click the **Refresh** button to refresh the last update.

3.1.2 Administration

Click the **Administration** option on the left frame to assign/change the setting (See Figure 3.4).

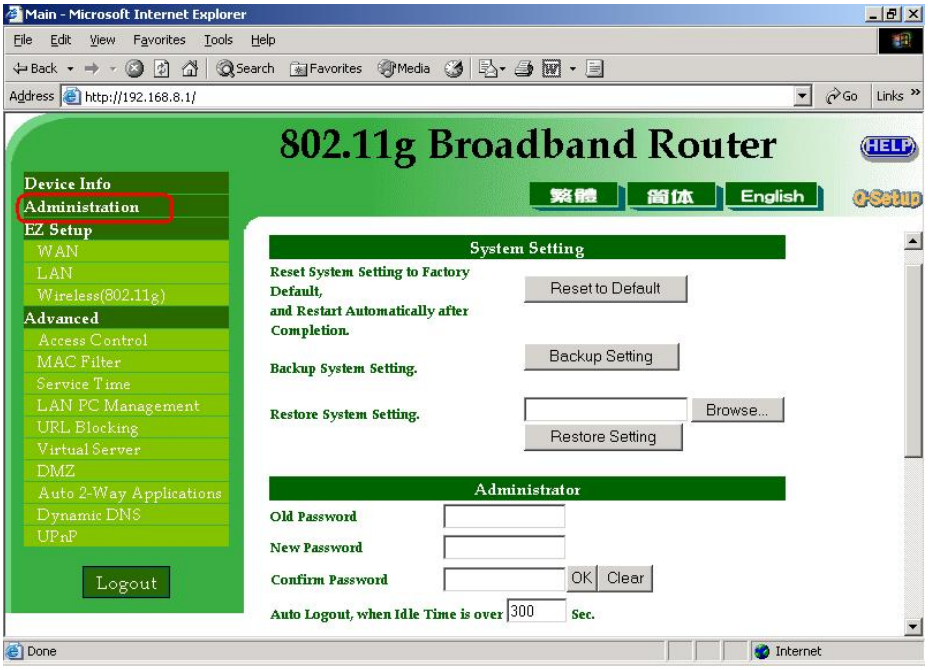


Figure 3.4 Administration Page

System Setting:

Reset to Default Reset system settings back to factory defaults, and restart automatically after completion.

Backup Setting Save the current system settings to a file.

Restore Setting Restore settings from a saved backup configuration file. When completed, the router will restart automatically.

Note:

The router allows restore system setting only when the backup setting file is created by the same firmware version. Otherwise it will deny the restore operation for reliability consideration.

Administrator:

Change Password Type in your old password, new password and confirm new password again. Then click **OK** to send this request.

Auto Logout Whenever administrator is idle for more than a specified time (default is 300 seconds). This is for security consideration.

Upgrade Firmware:

Click **Browse** to choose the correct firmware upgrade file (*.upg), and then click **Go** to send

this request. After about 20-30 seconds, the router will restart automatically.

Check the firmware version on **Device Info** page to confirm that the upgrade process was successful.

Miscellaneous Commands:

View System Event Log	The router records lots of system events, such as system start, administrator login/logout, dial/hang-up, and hacker intrusion event, etc. In addition, it stamps the date/time of each event.
Clone MAC	Duplicate the MAC address of administrator's PC into WAN MAC of the router.
Restart System	Force the router to restart immediately.

Click **View System Event Log** to browse the log record (Figure 3.5).

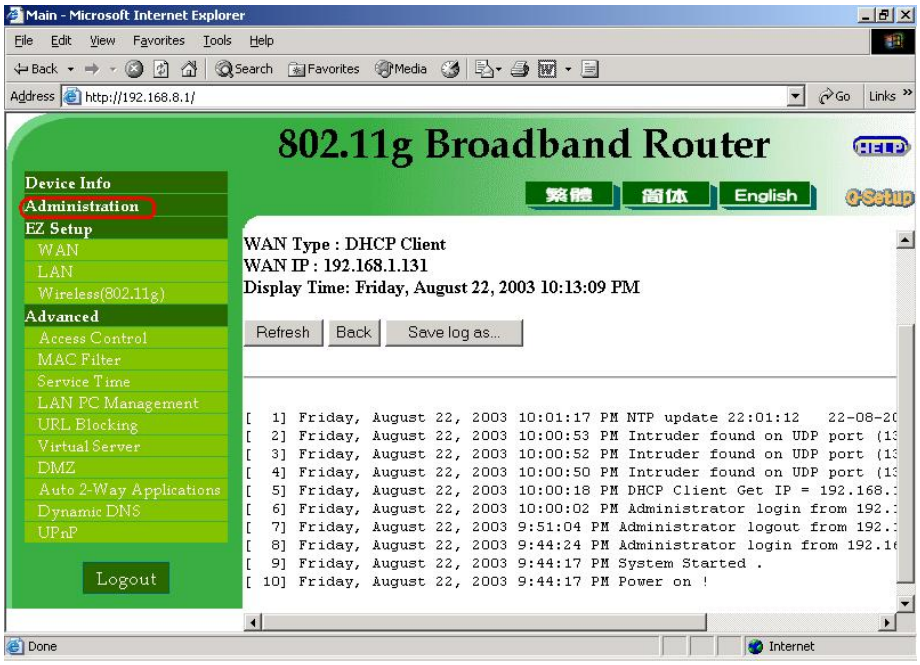

Main - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://192.168.8.1/
802.11g Broadband Router
Device Info
Administration
EZ Setup
WAN
LAN
Wireless(802.11g)
Advanced
Access Control
MAC Filter
Service Time
LAN PC Management
URL Blocking
Virtual Server
DMZ
Auto 2-Way Applications
Dynamic DNS
UPnP
Logout
繁體
簡体
English
WAN Type : DHCP Client
WAN IP : 192.168.1.131
Display Time: Friday, August 22, 2003 10:13:09 PM
Refresh
Back
Save log as...
[1] Friday, August 22, 2003 10:01:17 PM NTP update 22:01:12
[2] Friday, August 22, 2003 10:00:53 PM Intruder found on UDP port
[3] Friday, August 22, 2003 10:00:52 PM Intruder found on UDP port
[4] Friday, August 22, 2003 10:00:50 PM Intruder found on UDP port
[5] Friday, August 22, 2003 10:00:18 PM DHCP Client Get IP = 192.168.
[6] Friday, August 22, 2003 10:00:02 PM Administrator login from 192.
[7] Friday, August 22, 2003 9:51:04 PM Administrator logout from 192.
[8] Friday, August 22, 2003 9:44:24 PM Administrator login from 192.
[9] Friday, August 22, 2003 9:44:17 PM System Started .
[10] Friday, August 22, 2003 9:44:17 PM Power on !
Done
Internet

Figure 3.5 System Event Log

Note:

This function provides administrator a convenient diagnostic method for troubleshooting. Furthermore, it also provides detailed intruder/hacker information.

Refresh	Update these events.
Back	Back to the Administration page.
Save log as…	Save system event log to a file.

3.1.3 Quickly Setup

Click the **Q-Setup** if you want to quickly set up the router for use with a cable/DSL modem.

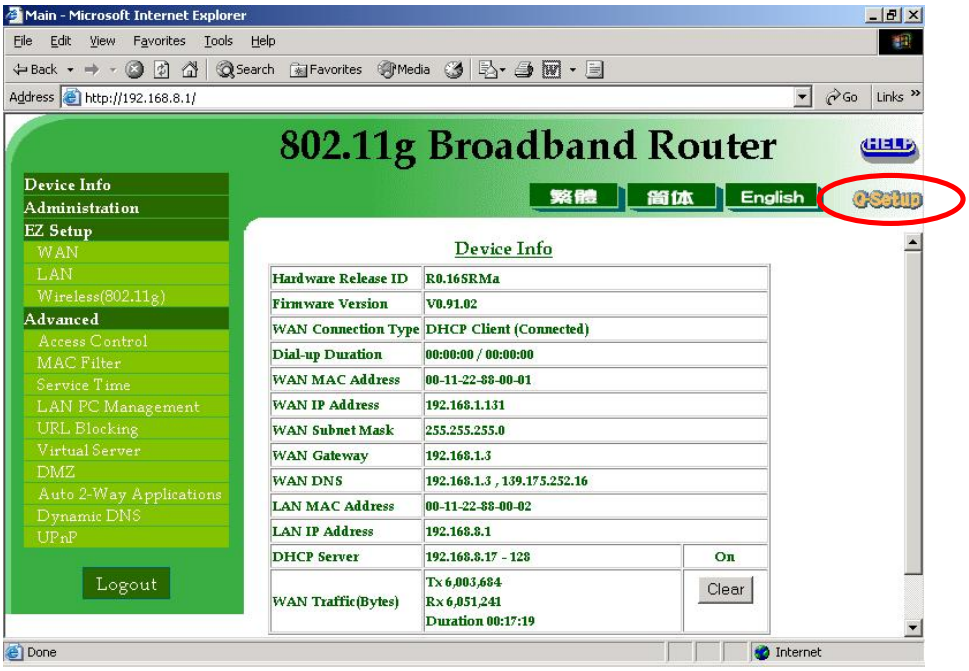


Figure 3.6 Quickly Setup

Time Zone

System Time Zone Select your local time zone from the drop-down list. This setting is used for the blocking schedule and for log events record.

Daylight Saving Check this box if your local time zone is currently under daylight savings time. Enable Daylight Saving will cause one hour to be added to the standard time.

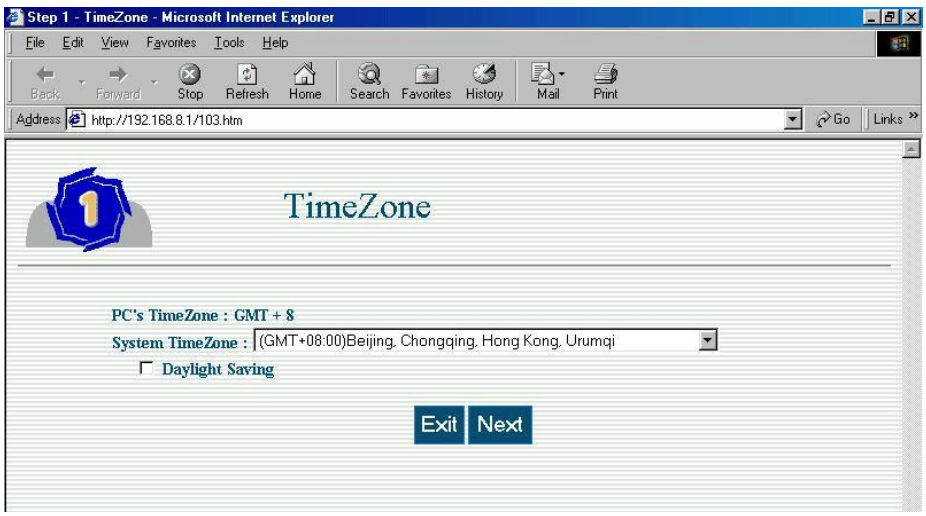


Figure 3.7 System Time Zone

WAN Type

There are four types of WAN connection – Static, DHCP client, PPPoE and PPTP client. Select the WAN connection type you have and click **Next** (Figure 3.8).

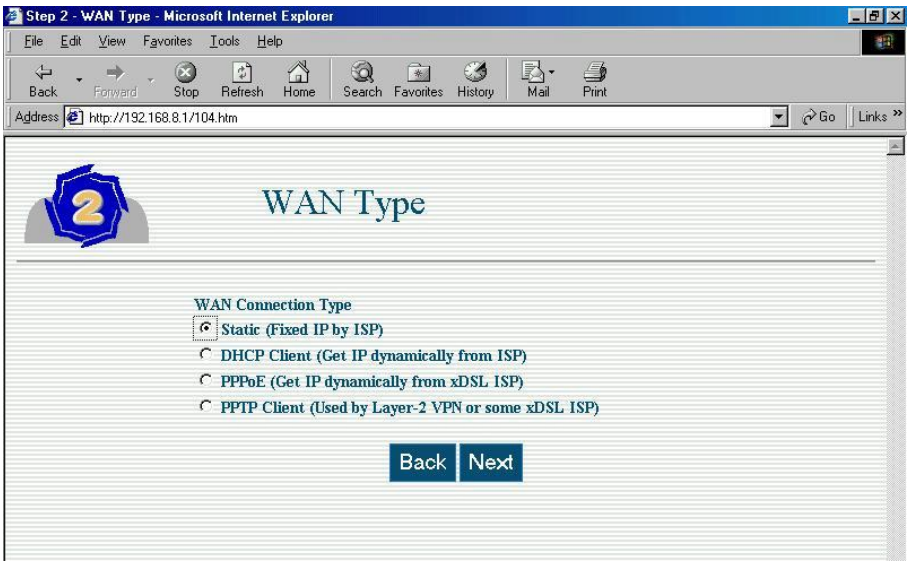

Step 2 - WAN Type - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print
Address http://192.168.8.1/104.htm
Go Links
WAN Type
WAN Connection Type
Static (Fixed IP by ISP)
DHCP Client (Get IP dynamically from ISP)
PPPoE (Get IP dynamically from xDSL ISP)
PPTP Client (Used by Layer-2 VPN or some xDSL ISP)
Back Next

Figure 3.8 WAN Type

A. Static

Some DSL Internet Service Providers may assign a static IP address. If you have been provided with this information, choose this option and enter the assigned IP address, subnet mask, gateway IP address and DNS IP addresses. Click **Done** to complete the setup (Figure 3.9).

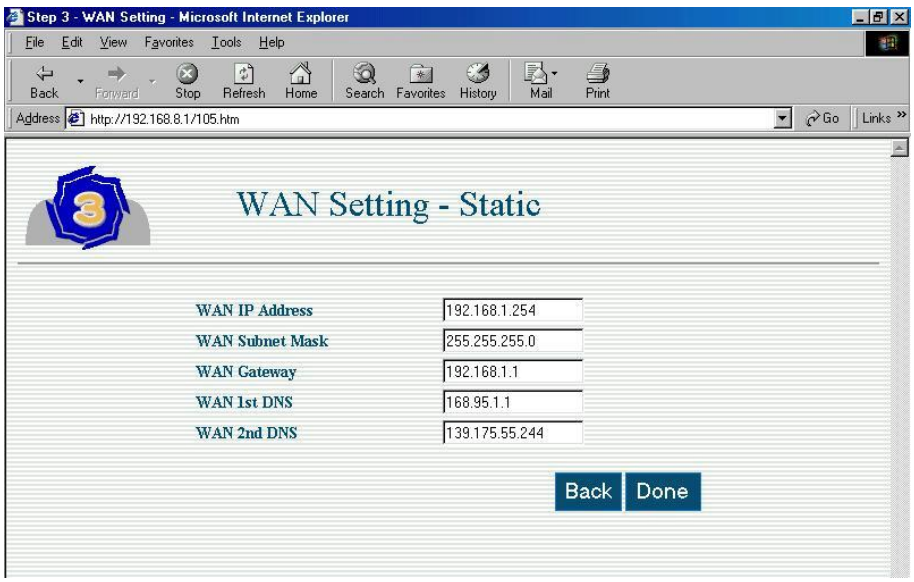

Step 3 - WAN Setting - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print
Address http://192.168.8.1/105.htm
Go Links
WAN Setting - Static
WAN IP Address 192.168.1.254
WAN Subnet Mask 255.255.255.0
WAN Gateway 192.168.1.1
WAN 1st DNS 168.95.1.1
WAN 2nd DNS 139.175.55.244
Back Done

Figure 3.9 WAN Setting – Static

B. DHCP Client

DHCP Client connection means your ISP will dynamically assign the IP address and other settings. The **Domain Name** and **Host Name** are optional, but may be required by some ISPs. Click **Done** to complete the setting (Figure 3.10).

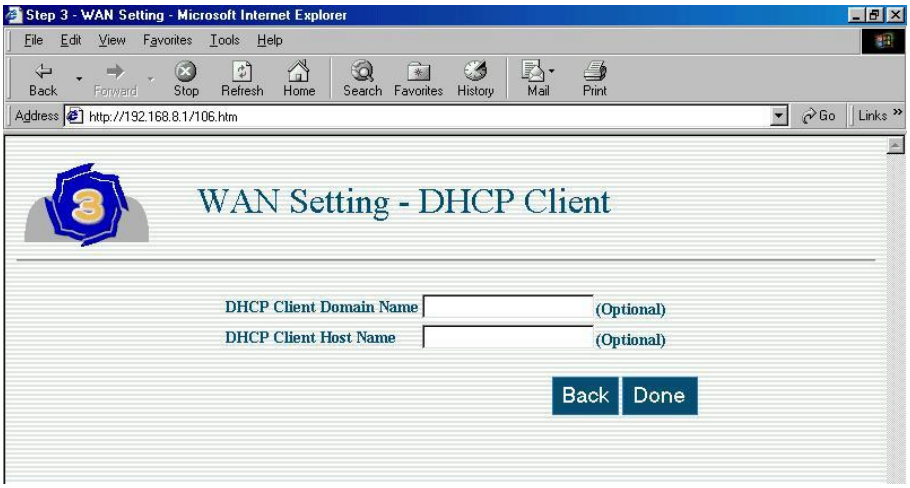

Step 3 - WAN Setting - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print
Address http://192.168.8.1/106.htm
Go Links
WAN Setting - DHCP Client
DHCP Client Domain Name (Optional)
DHCP Client Host Name (Optional)
Back Done

Figure 3.10 WAN Setting – DHCP Client

C. PPPoE

Enter **PPPoE Account** and **PPPoE Password** provided by your ISP. The **PPPoE Service Name** is optional, it may be required by some ISPs. Enable **Dial on Demand** automatically establish the Internet connection as soon as you attempt to access Internet. Enable **Auto-disconnect** if you want to disconnect your Internet connection automatically when it is idle more than a period of time.

Click **Done** to complete the setting (Figure 3.11).

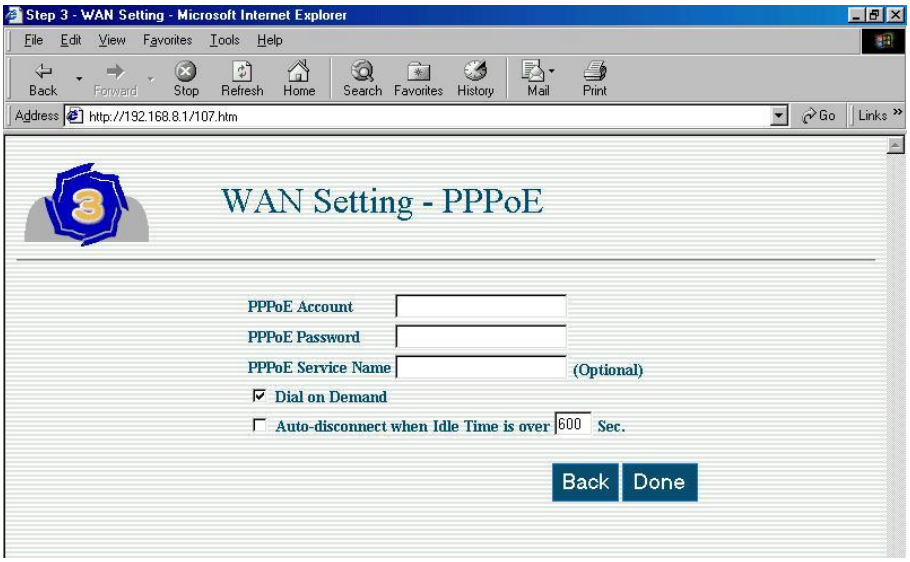

Step 3 - WAN Setting - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print
Address http://192.168.8.1/107.htm
Go Links
WAN Setting - PPPoE
PPPoE Account
PPPoE Password
PPPoE Service Name (Optional)
Dial on Demand
Auto-disconnect when Idle Time is over 600 Sec.
Back Done

Figure 3.11 WAN Setting – PPPoE

D. PPTP Client

Point-to-Point Tunneling Protocol is a common connection method used for xDSL connections in Europe. It can be used to join different physical networks using the Internet as an intermediary. Please check your ISP for details.

Where

- **My IP address** and **Server IP address** are the router (PPTP client) and ADSL Modem (PPTP server) IP address respectively.
- **My Gateway** is optional if PPTP client and server are in the same subnet. For Layer-2 VPN application, this field is necessary typically.
- The **PPTP Account** and **PPTP Password** are provided by ISP.
- The **PPTP connection ID** is left blank for most applications. Check with your ISP for correct setting if there are some problems.
- **Dial on Demand**: Enable this option to automatically establish the Internet connection as soon as you attempt to access Internet.
- **Auto-disconnect**: Enable this option if you want to disconnect your Internet connection automatically when it is idle more than a period of time.

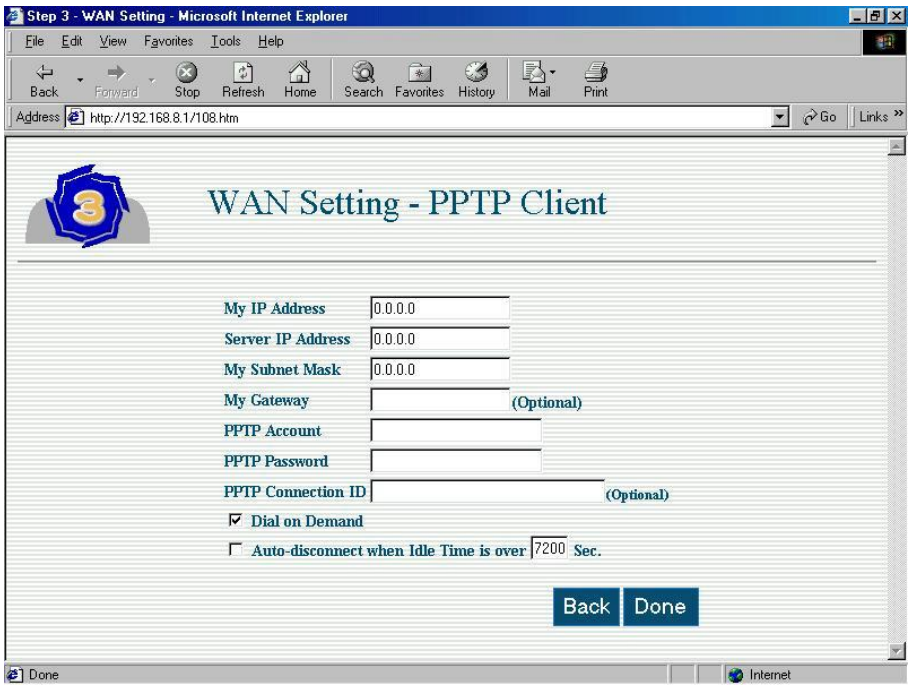

Step 3 - WAN Setting - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print
Address http://192.168.8.1/108.htm
Go Links
WAN Setting - PPTP Client
My IP Address 0.0.0.0
Server IP Address 0.0.0.0
My Subnet Mask 0.0.0.0
My Gateway (Optional)
PPTP Account
PPTP Password
PPTP Connection ID (Optional)
Dial on Demand
Auto-disconnect when Idle Time is over 7200 Sec.
Back Done
Done
Internet

Figure 3.12 WAN setting – PPTP Client

Click **Done** to complete the setting (Figure 3.12).

3.1.4 Online Help

Click the **HELP** icon to view the router's online help.

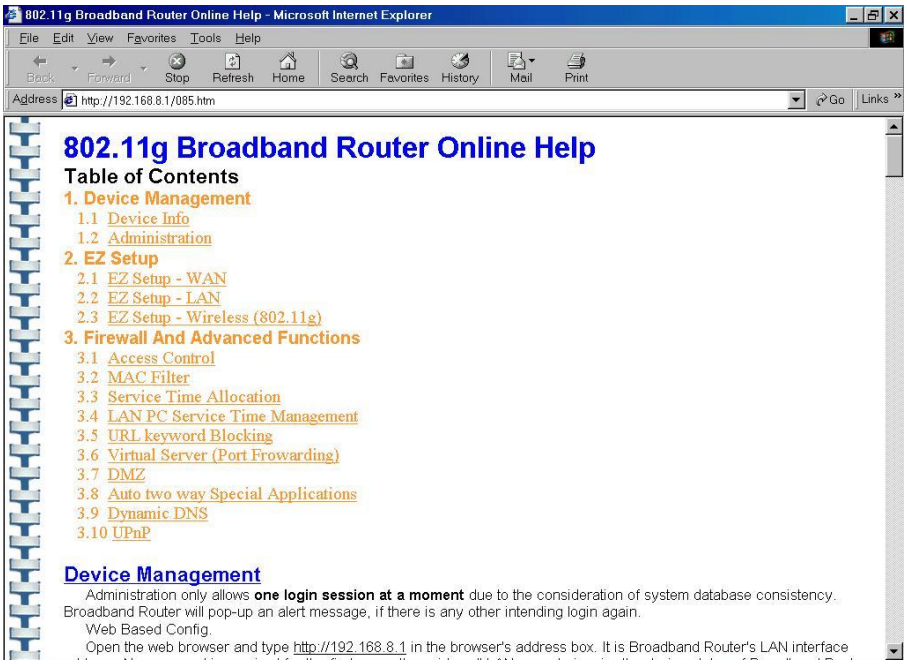

802.11g Broadband Router Online Help - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print
Address http://192.168.8.1/085.htm
Go Links
802.11g Broadband Router Online Help
Table of Contents
1. Device Management
1.1 Device Info
1.2 Administration
2. EZ Setup
2.1 EZ Setup - WAN
2.2 EZ Setup - LAN
2.3 EZ Setup - Wireless (802.11g)
3. Firewall And Advanced Functions
3.1 Access Control
3.2 MAC Filter
3.3 Service Time Allocation
3.4 LAN PC Service Time Management
3.5 URL keyword Blocking
3.6 Virtual Server (Port Frowarding)
3.7 DMZ
3.8 Auto two way Special Applications
3.9 Dynamic DNS
3.10 UPnP
Device Management
Administration only allows one login session at a moment due to the consideration of system database consistency.
Broadband Router will pop-up an alert message, if there is any other intending login again.
Web Based Config.
Open the web browser and type http://192.168.8.1 in the browser's address box. It is Broadband Router's LAN interface

Figure 3.13 Online help

3.1.5 EZ Setup - WAN

Click the **EZ Setup - WAN** option to specify the WAN connection type provided by your Internet Service Provider (See Figure 3.14).

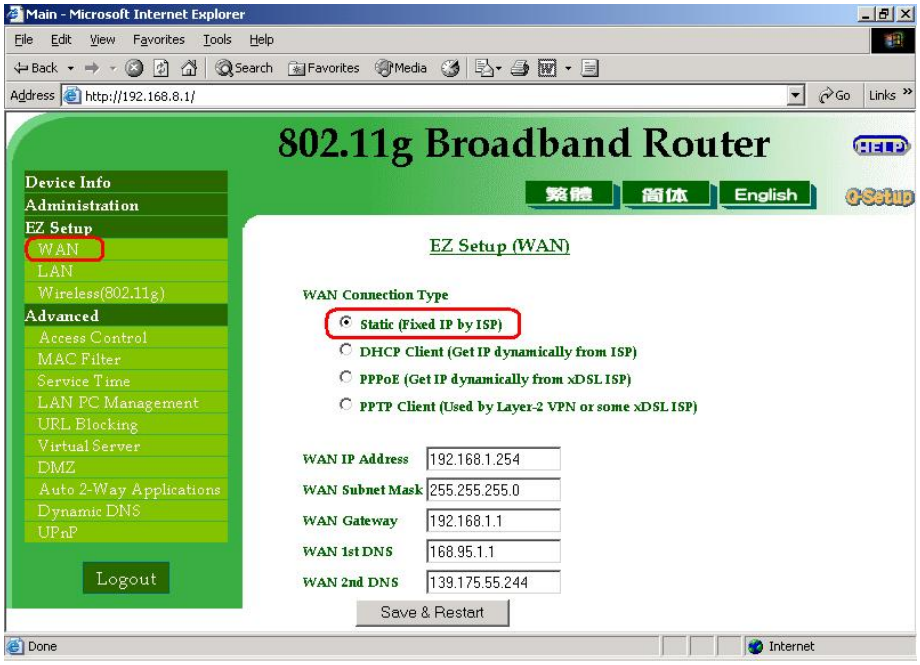


Figure 3.14 EZ Setup – WAN

Static IP

If your Internet Service Provider (ISP) has assigned a fixed IP address, choose the **Static** option (See Figure 3.14) and fill in the blanks according to the ISP provided information.

WAN IP Address	The router IP Address as seen by external users on the Internet.
WAN Subnet Mask	The router WAN IP address ranges. (e.g. 255.255.255.248 means the range of IP address is 8.)
WAN Gateway	ISP will provide the Gateway IP Address.
WAN 1st DNS	DNS (Domain Name Server). ISP will provide this address.
WAN 2nd DNS	The second DNS.

Click **Save & Restart** button to save this settings.

DHCP Client (Dynamic IP)

DHCP Client connection means your ISP will dynamically assign the IP address and other settings. The **Domain Name** and **Host Name** are optional, but may be required by some ISPs (See Figure 3.15).

Click **Save & Restart** button to save the settings.

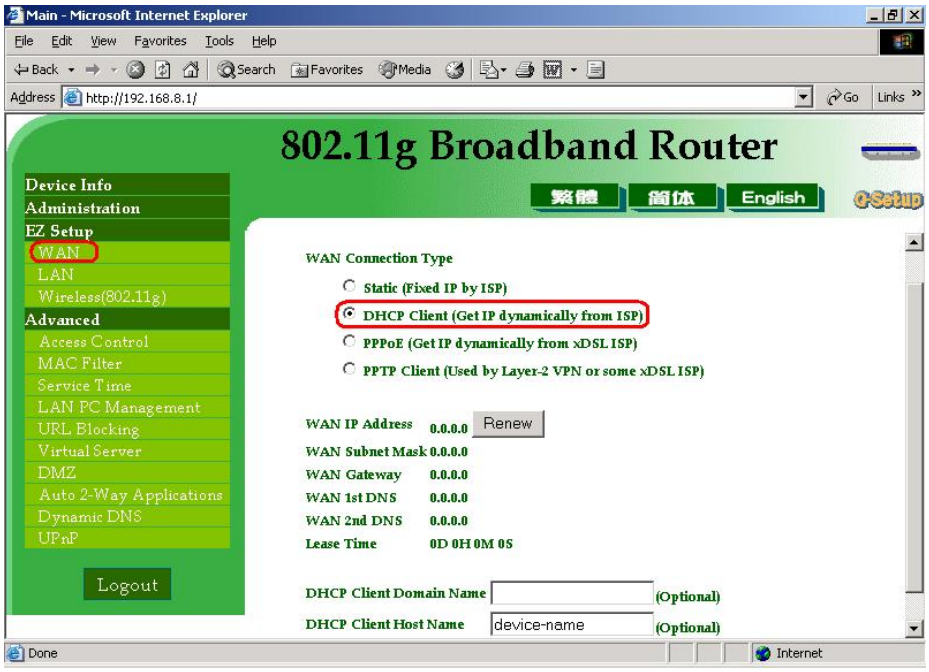


Figure 3.15 WAN Connection – DHCP Client

Note:

1. This connection type is more popular for Cable modem application.
2. After **Save & Restart**, once it is connected, the assigned IP setting could be inquired in **Device Info** page (refer to Section 3.1.1.)

PPPoE

Enter **PPPoE Account** and **PPPoE Password** provided by your ISP. The **PPPoE Service Name** is optional, it may be required by some ISPs.

Dial on Demand Enable this option to automatically establish the Internet connection as soon as you attempt to access Internet.

Auto-disconnect Enable this option if you want to disconnect your Internet connection automatically when it is idle more than a period of time.

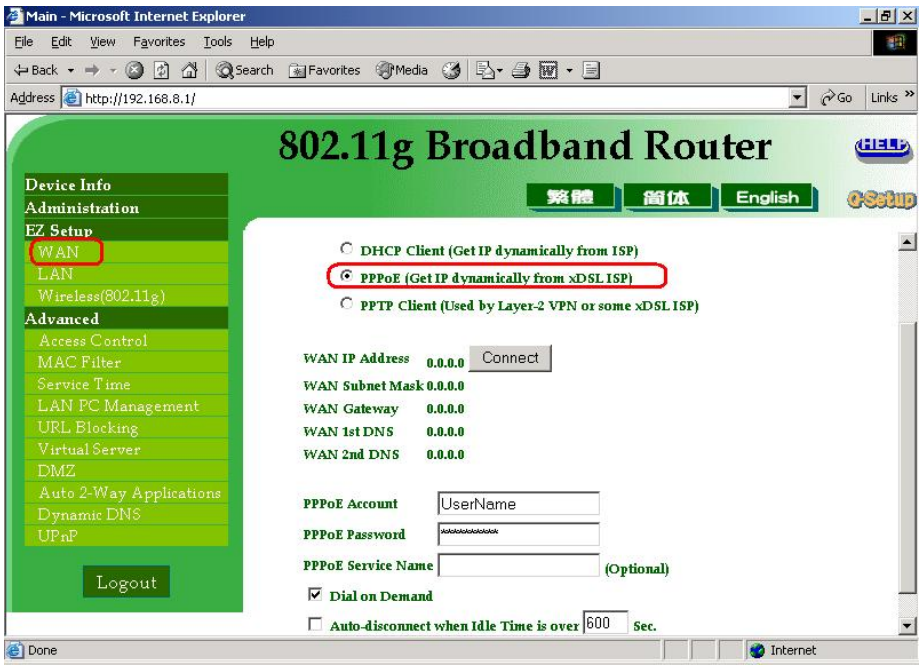


Figure 3.16 WAN Connection – PPPoE

Click the **Save & Restart** button to save the settings.

PPTP Connection

Point-to-Point Tunneling Protocol is a common connection method used for xDSL connections in Europe. It can be used to join different physical networks using the Internet as an intermediary. Please check your ISP for details.

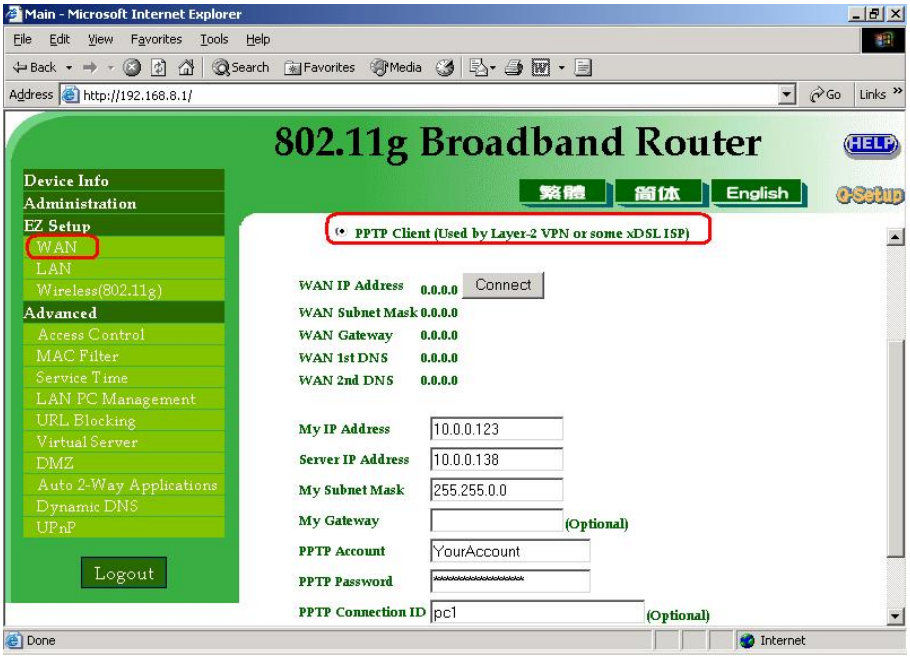


Figure 3.17 WAN Connection – PPTP

Where

- **My IP address** and **Server IP address** are the router (PPTP client) and ADSL Modem (PPTP server) IP address respectively.
- **My Gateway** is optional if PPTP client and server are in the same subnet. For Layer-2 VPN application, this field is necessary typically.
- The **PPTP Account** and **PPTP Password** are provided by ISP.
- The **PPTP connection ID** is left blank for most applications. Check with your ISP for correct setting if there are some problems.
- **Dial on Demand**: Enable this option to automatically establish the Internet connection as soon as you attempt to access Internet.
- **Auto-disconnect**: Enable this option if you want to disconnect your Internet connection automatically when it is idle more than a period of time.

Click **Save & Restart** button to save the settings.

3.1.6 EZ Setup - LAN

Click the **EZ Setup – LAN** option to setup LAN (See Figure 3.18).

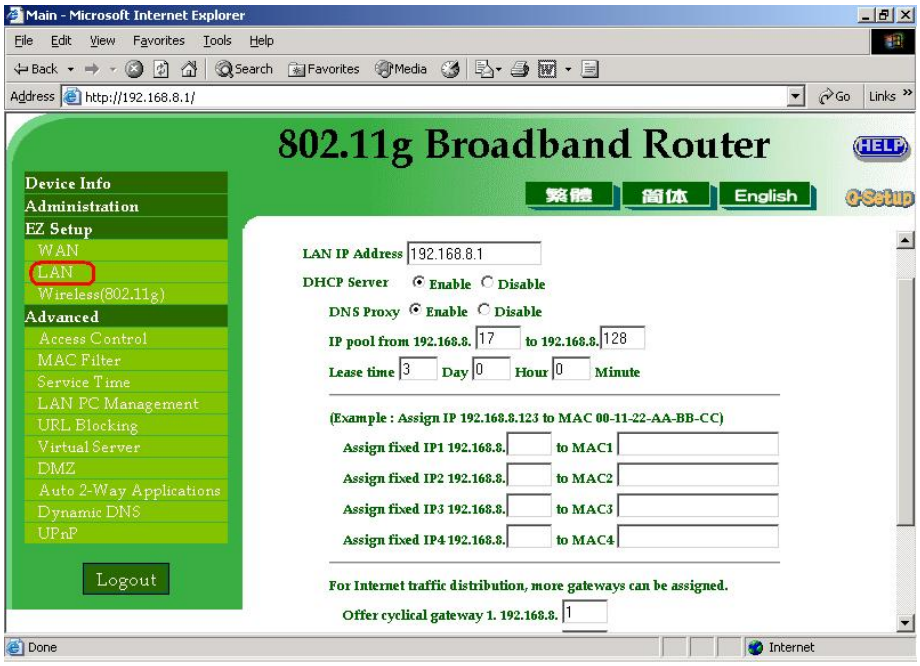


Figure 3.18 LAN Configuration

LAN IP Address The IP address of the router as it is seen on the internal LAN user.

Note:

If LAN IP is changed, the administrator might be lost connection with the router when they are not in the same LAN subnet. The administration does not work until they are in the same subnet again.

DHCP Server can be enabled (default) or disabled. They are described as follows.

1. DHCP Server Disabled

Disable DHCP Server function of the router. You have to manually configure LAN IP address.

2. DHCP Server Enabled

Choose this option if you want the router to assign IP to LAN computers automatically.

- **DNS Proxy**: LAN computers get their DNS service from the router first. The router will search the ISP's DNS automatically.
- **IP pool from 192.168.8.x to 192.168.8.x**: Whenever there is a request, the DHCP server will offer unused IP from the IP address pool to the requesting computer.

- **Lease time**: The assigned IP will be valid during the lease interval.
- **Assign fixed IP to MAC**: If there are some computers (such as a web/E-mail server) which will be assigned a fixed IP by DHCP server, you can set these computers with their own predefined IPs. These computers will be identified by their MAC addresses.

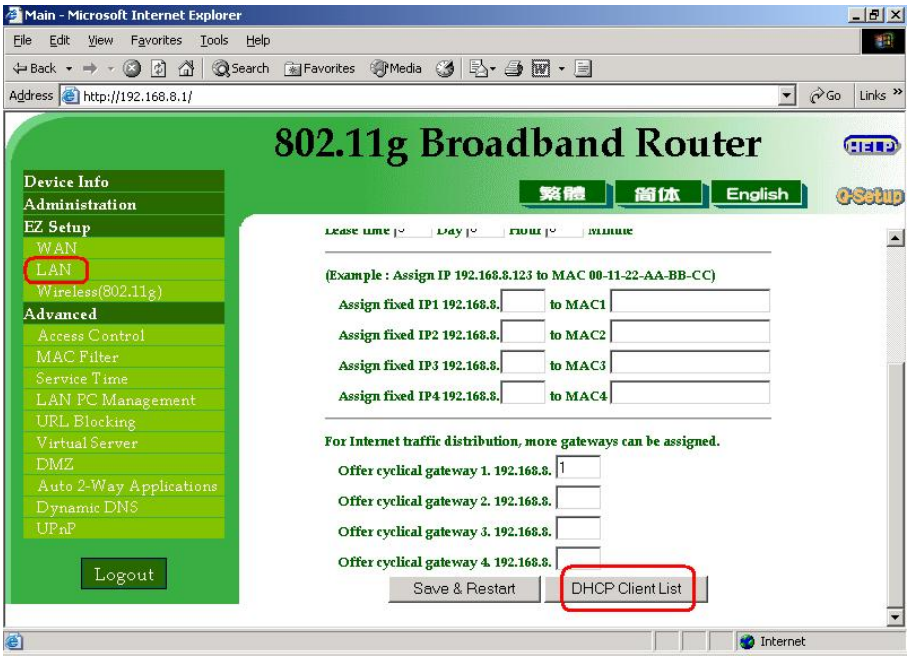
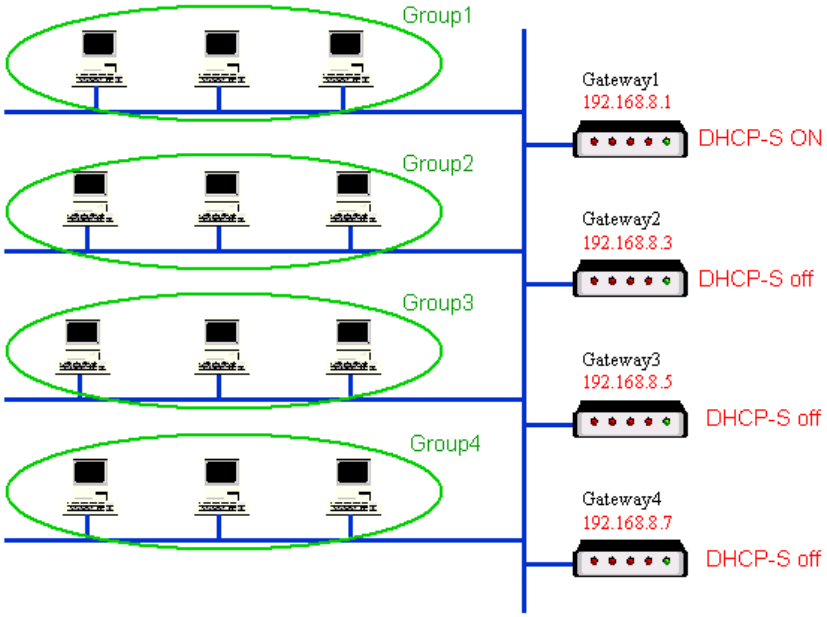


Figure 3.19 LAN Configuration

- **Offer cyclical gateway**: it is a very simple mechanism for Internet/WAN traffic distribution evenly among those routers (up to 4) within a network.

Note:

1. This application is used only for those network have more routers in the same subnet.
2. There is **one and only one DHCP server allowed in a specific subnet.** Please chooses either one gateway as DHCP server, the other must be disabled.



Click **Save & Restart** to save all those setting.

Click **DHCP Client List** to show DHCP Client list.

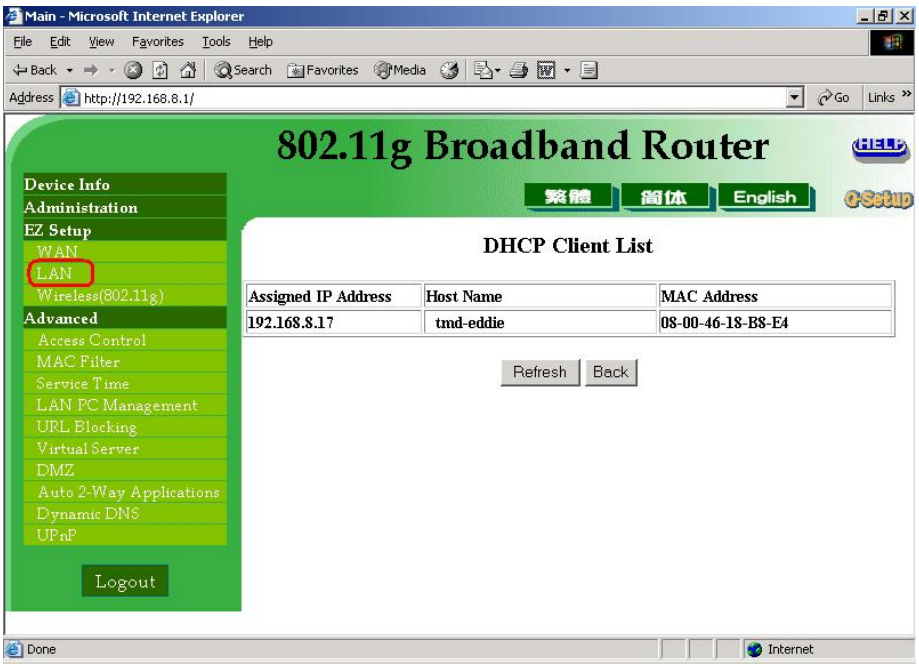


Figure 3.20 DHCP Client List

Click **Refresh** button to get the most updated client information.

Click **Back** button to return to the **EZ Setup – LAN** page.

3.1.7 EZ Setup – Wireless (802.11g)

Click the **Wireless (802.11g)** option to inquire/configure wireless LAN setting (Figure 3.21).

Wireless Info:

Displays WLAN information.

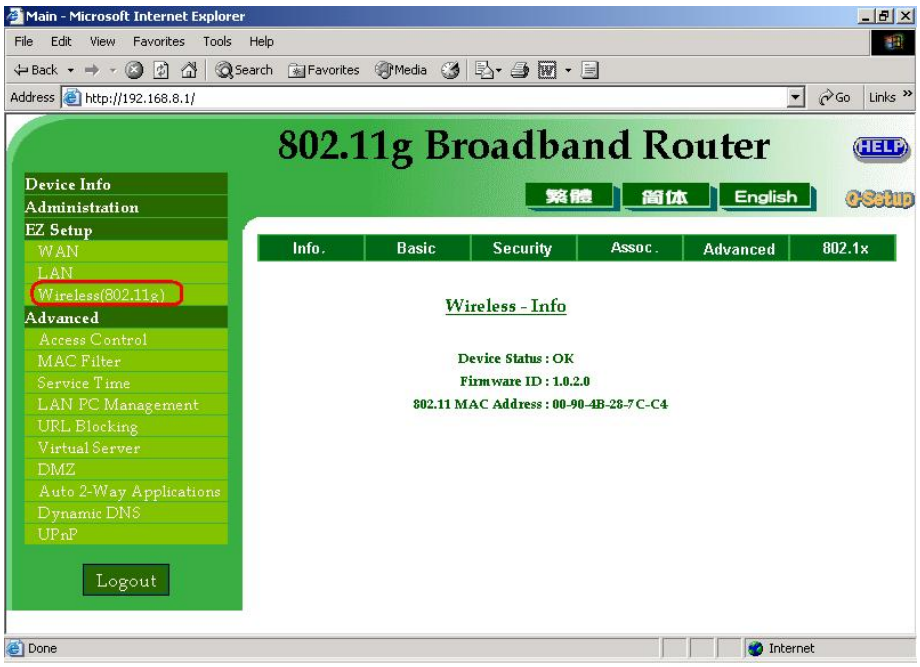


Figure 3.21 Wireless – Info.

Where:

Device Status

Indicates internal wireless 802.11g module status. Normally it is shown "**OK**". If it shows "**Failed**", it means the wireless interface is unavailable.

Firmware ID

Displays the version identification for internal wireless 802.11g module.

802.11 MAC Address

Shows the MAC address of internal wireless 802.11g module.

Basic:

Enter the basic/mandatory setting for 802.11g.

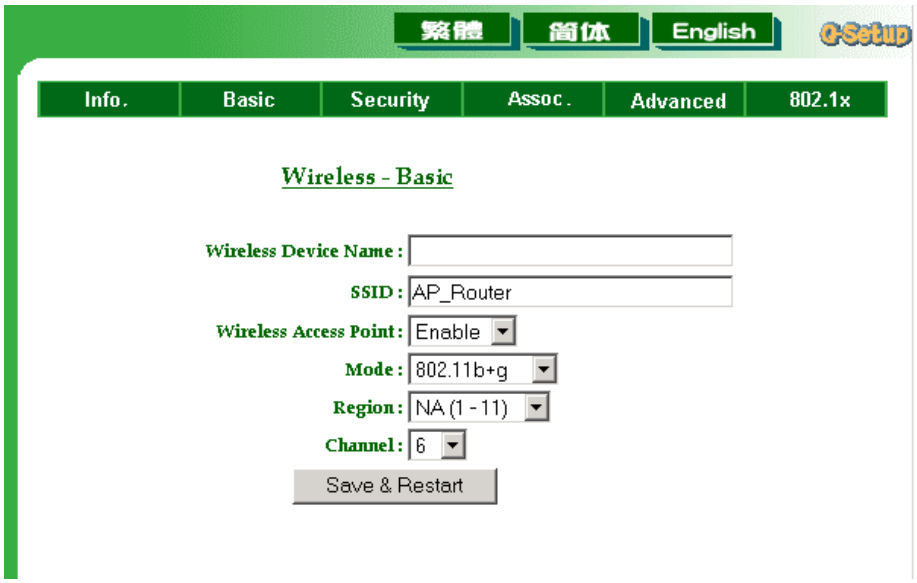


Figure 3.22 Wireless – Basic

Where:

Wireless Device Name

The field to store a descriptive/meaningful string used by the wireless window utility (like search or locating utility) to report which AP or AP router it is.

SSID (Service Set ID)

A unique ID shared by the same group wireless client PCs and one or more wireless AP (Access Point)/AP router.

Wireless Access Point

The Access Point function could be enabled/disabled. Sometimes it could be disabled temporarily for security consideration.

Mode

802.11b+g could achieve the most compatible application environment. However **802.11g only** will gain the best performance in throughput.

Region

Since the allowed RF band is not globally the same. Thus choose the region where it complies with your local regulation.

There are five region in the option list 1) North American. 2) ETSI: Pan Europe. 3) France 4) Spain. 5) Japan

Channel

Radio channels used by the wireless 802.11g module.

Security

Enter the WEP key and enable/disable security feature.

繁體
簡体
English
Q-Setup
Info.
Basic
Security
Assoc.
Advanced
802.1x
Wireless - Security
Disable Broadcast of SSID :
WEP Configuration
For 64 bit keys, you must enter 10 hexadecimal digits or 5 alphanumeric(ASCII) characters into the key fields.
For 128 bit keys, you must enter 26 hexadecimal digits or 13 alphanumeric(ASCII) characters into the key fields.
Leaving the key fields to blank means no change to the key.
WEP Enabled :
WEP Key Length : 64 bit key
PassPhrase :
Generate WEP Key
Hex Key
ASCII Key

Figure 3.23 Wireless – Security

Disable Broadcast of SSID

Option to hide the SSID in beacon, so that WLAN router cannot be found by a passive scan program/utility. This is used in a more secure application environment.

WEP Enabled

Enable/disable the Wired Equivalent Privacy security function.

WEP Key Length

Selects 64-bit or 128-bit WEP encryption. Be sure that the setting in router shall be the same as all wireless client PCs, otherwise the communication is impossible.

PassPhrase

Used to generate WEP-64 or WEP-128 key 1-4 automatically.

WEP key

For **64-bit** WEP encryption, a key of **10** hexadecimal characters in length must be filled in.

For **128-bit** WEP encryption, a key of **26** hexadecimal characters in length must be filled

in.. Be sure that the key in router shall be the same as all wireless client PCs, otherwise the communication is impossible.

WEP key to use

Selects one of four key sets to be used for encryption. To connect to a Wi-Fi compliant wireless device, key #1 must be selected.

Authentication

Selects the mechanism of **shared** key, **open** system or **both** authentication algorithm

Association

The upper list shows all MAC address of associated with router currently.

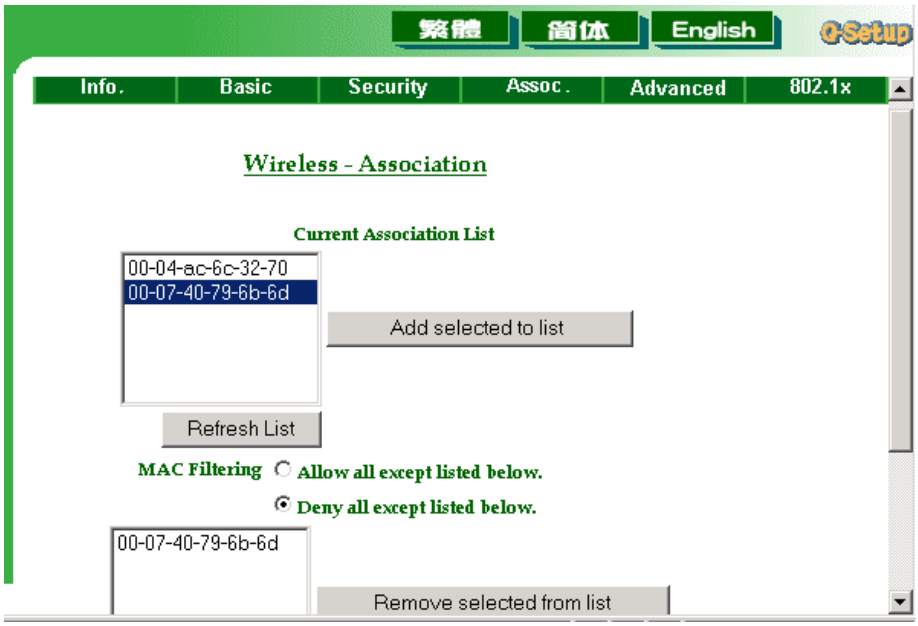


Figure 3.24 Wireless – Association

The lower list is a MAC address filtering function. There are two mechanism are provided:

1) Allow all wireless client PCs except the following MAC address stations.
2) Deny all wireless client PCs except the following MAC address stations.

The allowed/denied list could be filled from the upper associated MAC list or key in manually.

Advanced

Figure 3.25 Wireless – Advanced

Max. Connected Stations

Specify the maximum allowed wireless stations to the router. It is used to limit the wireless user number at most.

Fragmentation Threshold

This value specifies the maximum size for a packet before data is fragmented into multiple packets. It should remain at its default setting of 2346. Only minor reductions are recommended.

RTS Threshold

This value should remain at its default setting of 2347. Only minor reductions are recommended.

Beacon Period

This value indicates the frequency interval of the Beacon signal.

DTIM Period

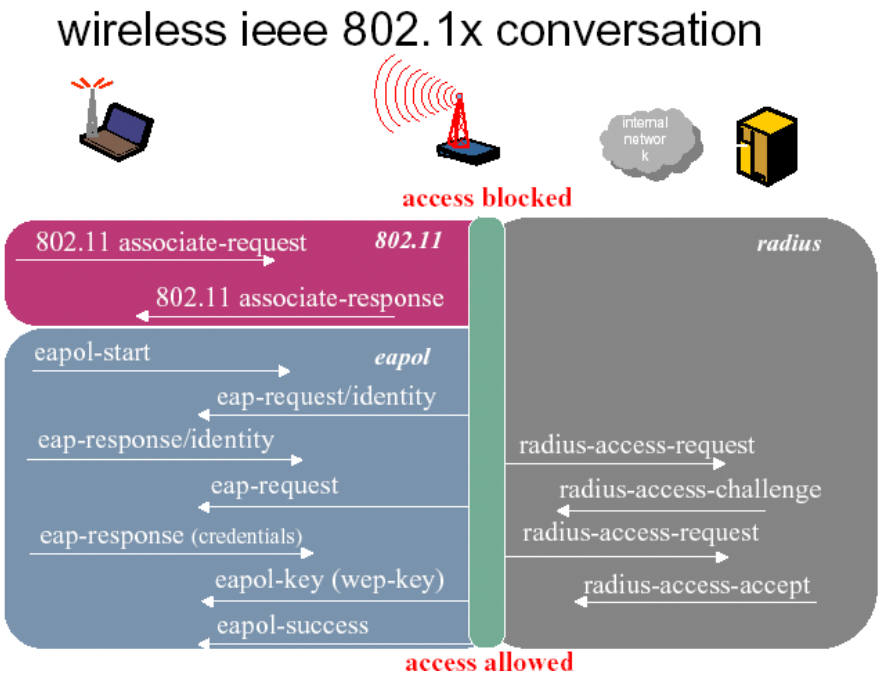
This value, between 1 and 255 ms, indicates the interval of Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing the clients of the next window for listening to broadcast and multicast message.

Preamble Type

Choose **long**, **short** and **dynamic** preamble in physical layer. Default is **dynamic** preamble.

802.1x

IEEE 802.1x is a more secure, user level oriented, authentication method to the wire connection. (Please refer to following diagram)



According to the above configuration, the RADIUS server is necessary and more important.

Figure 3.26 Wireless – 802.1x

Note:

1. Once the 802.1x function is ON, the RADIUS server must be setup correctly. Otherwise none of the mobile client could associate with the router successfully.
2. Since there are lot of authentication standard (e.g. MD5, TLS, TTLS, PEAP, LEAP) used in the different RADIUS. Currently, MD5, TLS and PEAP are supported with Microsoft RADIUS server.

A MD5 tiny server is built-in with the router to simplify the 802.1x application requirement. Since it could provide the same secure authentication mechanism, and it could work even the RADIUS server is absent environment. Certainly, the MD5 authentication is supported only.

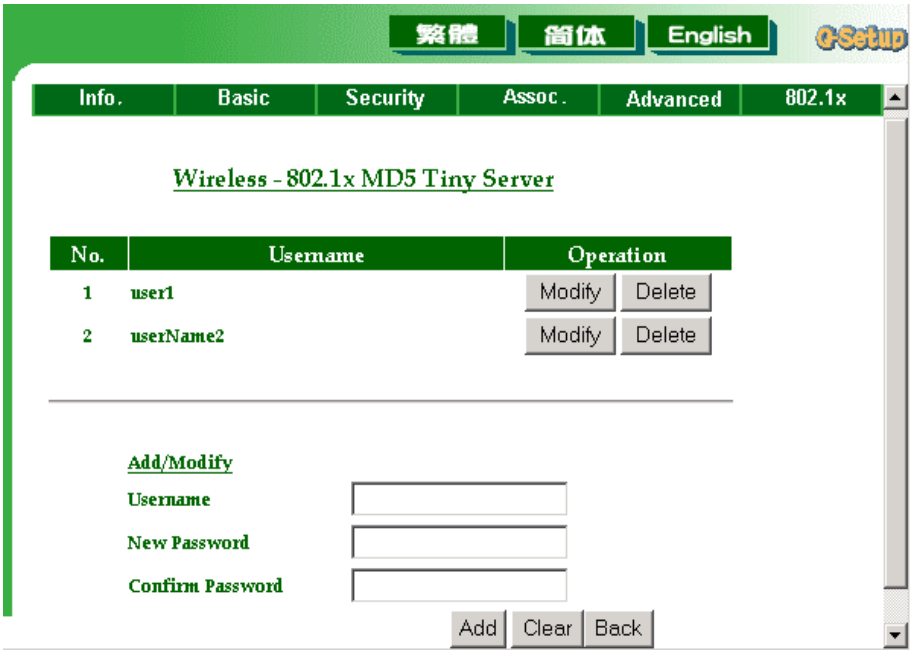


Figure 3.27 Wireless – 802.1x MD5 Tiny Server

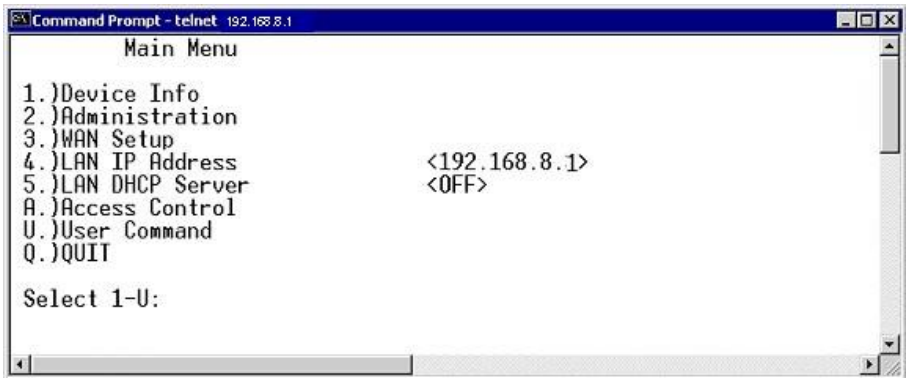
3.2 Telnet Configuration

The router also provides the Command Line Interface (CLI) for simple configuration. It is implemented by the Telnet protocol. Thus it just like the Sec. 3.2 Web configuration, the TCP/IP network should be setup correctly. Then it is possible to use the Telnet configuration.

In general, the Telnet configuration is menu-driven operation to simplify the user interface. As a result, only basic configuration function is implemented (for firewall advanced and wireless setting, please use WEB configuration directly).

1. On the Windows taskbar, click **Start/Program/Command Prompt**
2. Type **telnet 192.168.8.1** and press the <Enter> key to enter the configuration main menu.

3. Enter the password to login (Default is **admin**). Then the main menu is shown below.
4. Select the item number to enter.



4. Firewall and Advanced Functions

Besides the native protection features from NAT, the router provides lots of advanced functions which are popular in most firewall devices such as deny PING, MAC address filtering, IP address filtering, TCP/UDP service port blocking, URL keyword blocking, virtual server, DMZ and intrusion event log. (It is stored into internal buffer. Please refer to Section 3.1.2).

4.1 Access Control

Access control allows you to control the WAN-to-LAN or LAN-to-WAN access capability (See Figure 4.1).

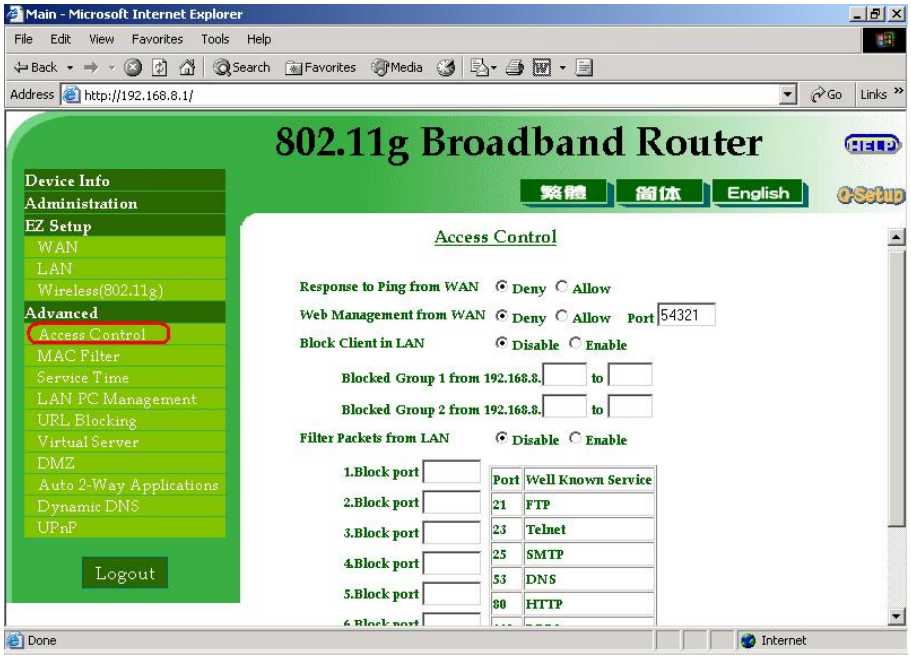


Figure 4.1 Access Control

Response to Ping from WAN

Prevents the router from responding to any PING request on the WAN port. This is very useful to prevent Internet intruders/hackers from probing computer. Most likely, hackers will not have any willing to start attack due to no PING response.

Web Management from WAN

This function allows administrator to configure the router through Internet. In order to reserve HTTP service (port 80) used for virtual server function, this remote web

administration function utilizes another port **54321** instead (e.g., http://211.79.244.45:**54321**).

Block Client in LAN

This function is used to inhibit some LAN clients (by IP address) from accessing Internet resources. Since all inhibiting LAN clients are recognized by its IP address, no matter the inhibiting LAN client's IP address is assigned by DHCP server or manual setting, this function always works well.

Filter Packets from LAN

This function allows administrator to inhibit a LAN user from using some Internet services.

For example, if the router is used in SOHO environment and the administrator wants to inhibit LAN user from using Telnet services (like BBS, on-line chat…), then it is easily achieved by blocking all packets to service port 23.

Another example, blocking service port 110 (POP3) will inhibit LAN user from checking/retrieving outside Internet e-mail account periodically. This is very useful when WAN connection type is Dial-on-Demand (like PPPoE/PPP). It can prevent the LAN users from periodical e-mail checking and causing the router keep WAN connection alive forever. Certainly, in this situation the LAN users can only use e-mail server inside (POP3 server exist in LAN).

4.2 MAC Filter

MAC Filter allows administrator to control the LAN client computers to access Internet with a robust method (by hardware oriented MAC address).

There are two mechanisms are supported.

1. All LAN client computers **can** access Internet, except the MAC address listed in the table.
2. All LAN client computers **cannot** access Internet, except the MAC address listed in the table.

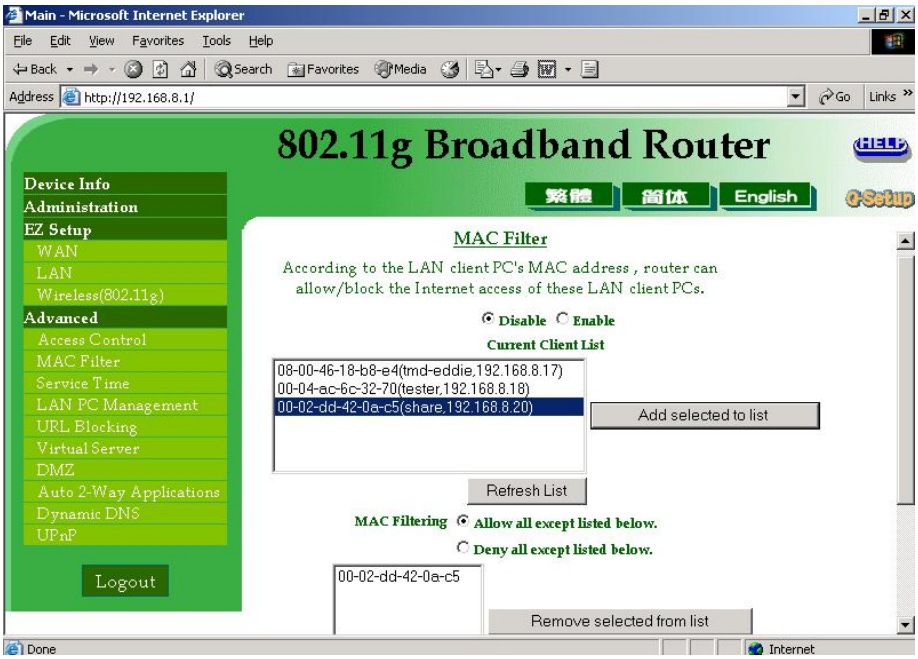


Figure 4.2 MAC Filter

4.3 Service Time Allocation

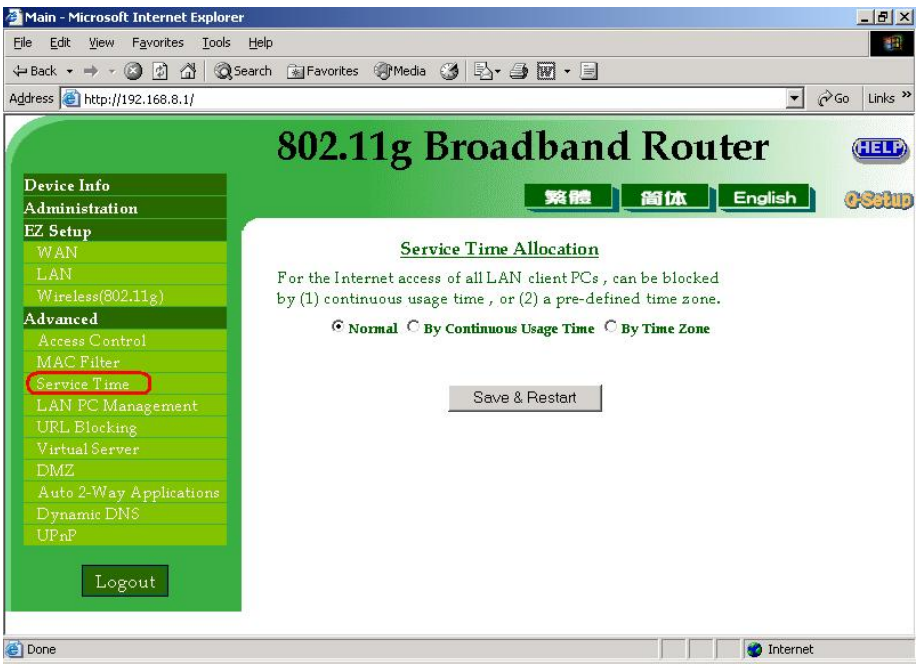


Figure 4.3 Service Time Allocation

For the Internet access of all LAN client PCs, can be blocked by (1) continuous usage time, or (2) a pre-defined time zone.

By Continuous Usage Time

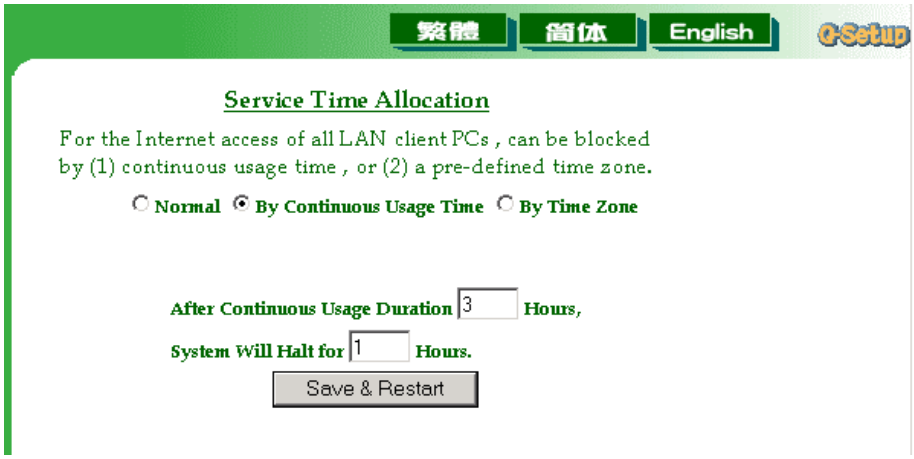

繁體
簡体
English
Q-Setup
Service Time Allocation
For the Internet access of all LAN client PCs , can be blocked by (1) continuous usage time , or (2) a pre-defined time zone.
Normal
By Continuous Usage Time
By Time Zone
After Continuous Usage Duration 3 Hours,
System Will Halt for 1 Hours.
Save & Restart

Figure 4.4 Time Allocation by Continuous Usage Time

One is to specify the **maximum continuous service period** (See Figure 4.4). This is primarily used for parental control in home application. It could protect children from surfing Internet continuously for more than a pre-defined period **X**. In the meanwhile, the router will stop service until period **Y** is expired (See Figure 4.5).

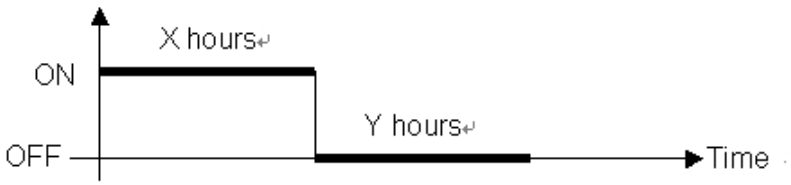


Figure 4.5 Stop Service Y Hours After X hours Service

By Time Zone

The other mechanism is simply dependent on a daily time zone. This means the router's LAN-to-WAN service is on or off according to a predefined daily schedule table (See Figure 4.6).

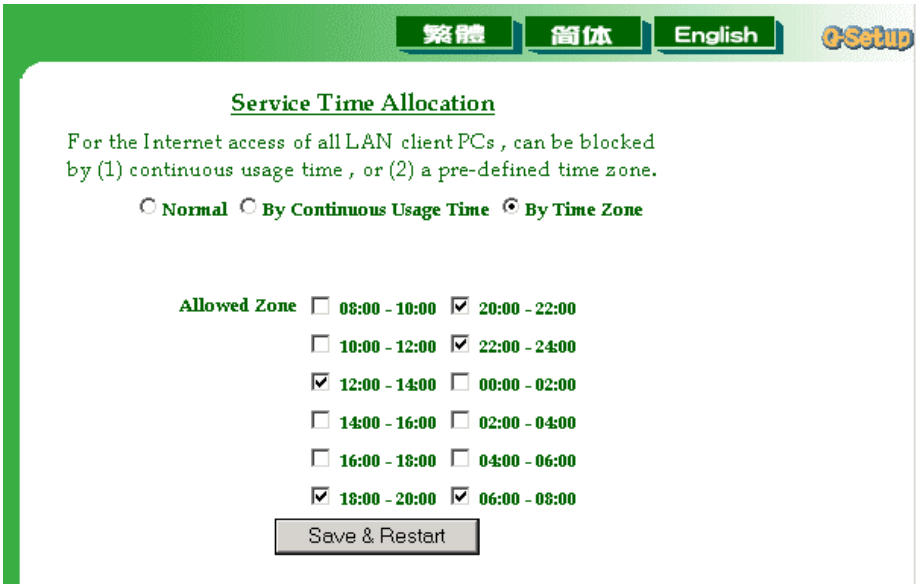


Figure 4.6 Time Allocation by Time Zone

4.4 LAN PC Management

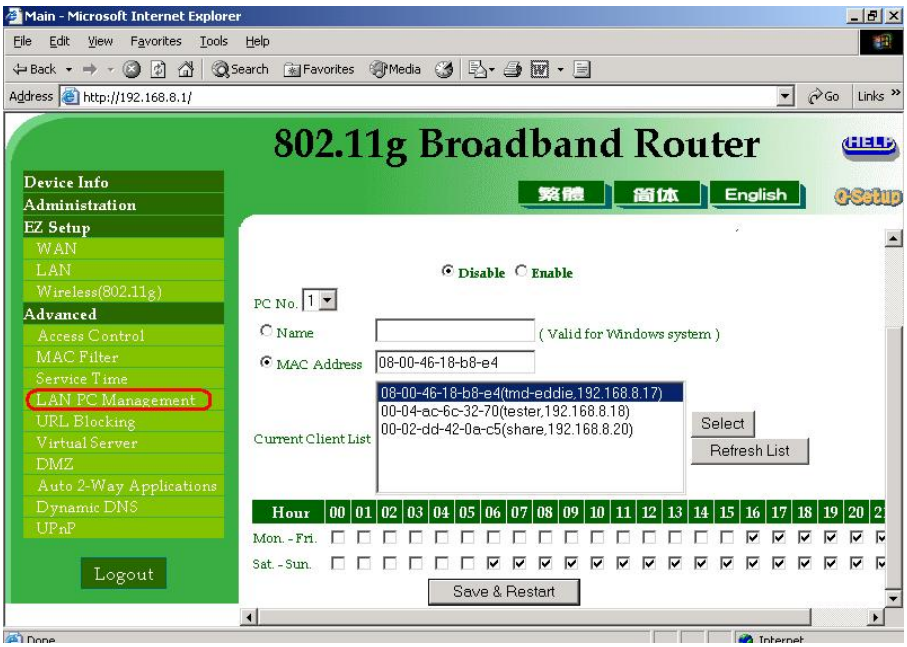


Figure 4.7 LAN PC Management

Besides the service time allocation mechanism, the router also provides another time-based management for each individual LAN client PCs (up to 8 PCs). Since each PC is identified uniquely by its hardware MAC address, and each PC has its own weekly timetable. As a result, it is useful for administrator to control a small group of PCs with a precise service time

schedule.

Click **Save & Restart** button to save the settings.

4.5 URL Blocking

Prevent any LAN client PC from accessing unwanted Internet site by partially matched URL keywords. Administrator could enter the URL keywords which website to be rejected. Then the router will reject all websites which URL names are matched or partially matched.

For example, if the keyword is **xyz**, then all www.**xyz**.com, ftp.**xyz**.com, **xyz.**abc.com… are all blocked.

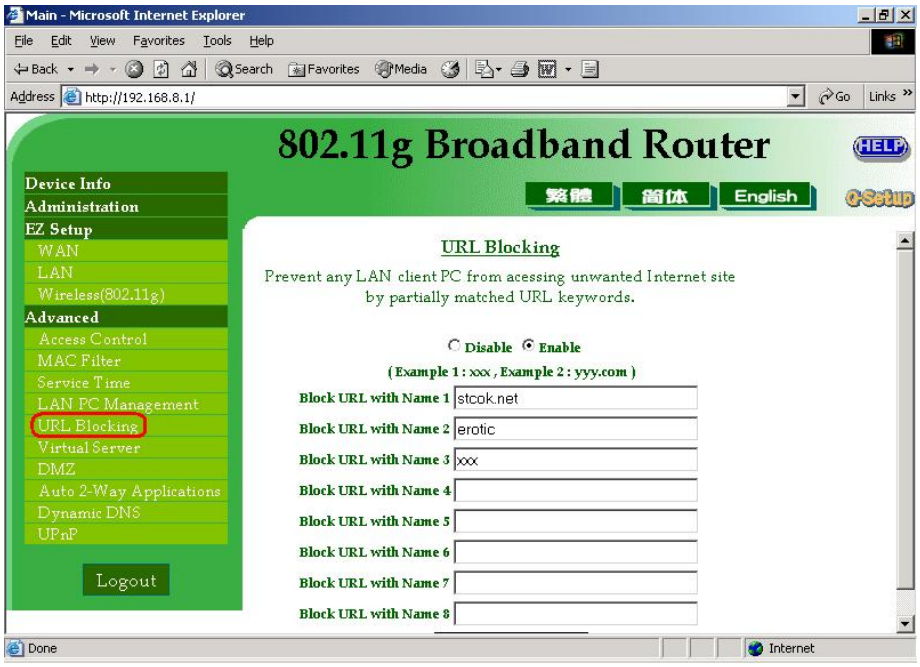


Figure 4.8 URL Blocking

Click **Save & Restart** button to save the settings.

4.6 Virtual Server

Generally NAT based router/firewall filters out all unrecognized packets from WAN in order to protect your Internal LAN computers; therefore all LAN computers behind the router are invisible to the outside Internet. However, some Internet servers (like WWW, FTP, E-mail...) should be visible and accessible by outside Internet. As a result, the router provides Virtual Server functions to meet such applications. In addition, it also protects the servers and all other computers in LAN simultaneously (See Figure 4.9).

Since all the Internet servers always handle the fixed TCP/UDP service port number (e.g., WWW is TCP/80, FTP is TCP/21...). Thus, any packet from WAN with **destination port number** is matched with the router virtual server's ports will be **forwarded to the pre-defined LAN's IP**. Certainly, the destination port number could be kept the same or mapped into another port for LAN.

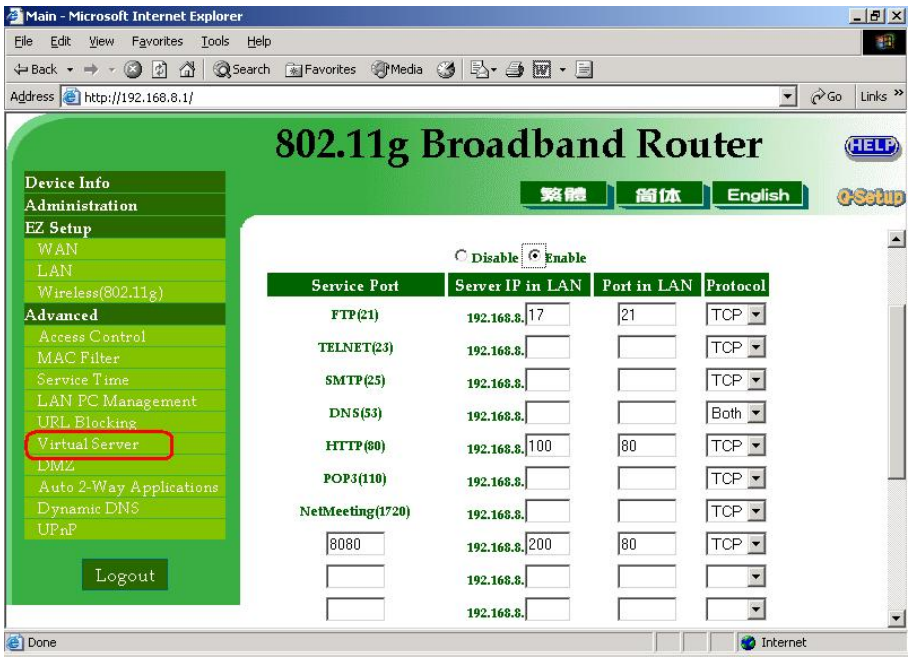


Figure 4.9 Virtual Server

For example, if you have an FTP server (port 21) at 192.168.8.5, a mail server (port 110) at 192.168.8.6, and a VPN server (port 1723) at 192.168.8.7, then you need to specify the virtual server as:

WAN IP + port 21 **è** 192.168.8.5 + port 21
WAN IP + port 110 **è** 192.168.8.6 + port 110
WAN IP + port 1723 **è** 192.168.8.7 + port 1723

Another example: if there are two Web servers in LAN (and installed by 2 different computers)

WAN IP + port 80 **è** 192.168.8.8 + port 80
WAN IP + port 80 **è** 192.168.8.9 + port 80

Please refer to Appendix A for some well-known service ports.

4.7 DMZ

DMZ (Demilitarized Zone) is a zone, which is not protected by firewall. It means all computers in DMZ are dangerous and subject to be attacked/accessed by Internet intruders/hackers. However, the advantage is that all computers in DMZ are totally exposed to Internet, thus all of them gain the full access privilege right to outside Internet. In such case, most Internet applications may be much more compatible with them (because there is not any interference from firewall function) (See Figure 4.10).

Currently there are more applications needs unrestricted 2-way Internet access and they open many TCP/UDP ports simultaneously (like video and/or audio conference, on-line gaming...). The router provides this feature to allow some computers in LAN to have unrestricted 2-way access privilege right. As a result, those computers in DMZ are more compatible with Internet applications. Certainly, they seem to be dangerous in comparison with those other computers in LAN.

The router generally allows a computer in LAN to be logically exposed to Internet with unrestricted 2-way communication capability. This is very useful whenever you encounter some incompatible issues (especially for online game or audio/video conference), most likely to turn on DMZ feature so that this problem can be avoided.

The single DMZ host (shown in Figure 4.8) is allowed due to the single WAN IP address condition. For example, WAN connection type is DHCP client, PPPoE, PPTP, or PPP.

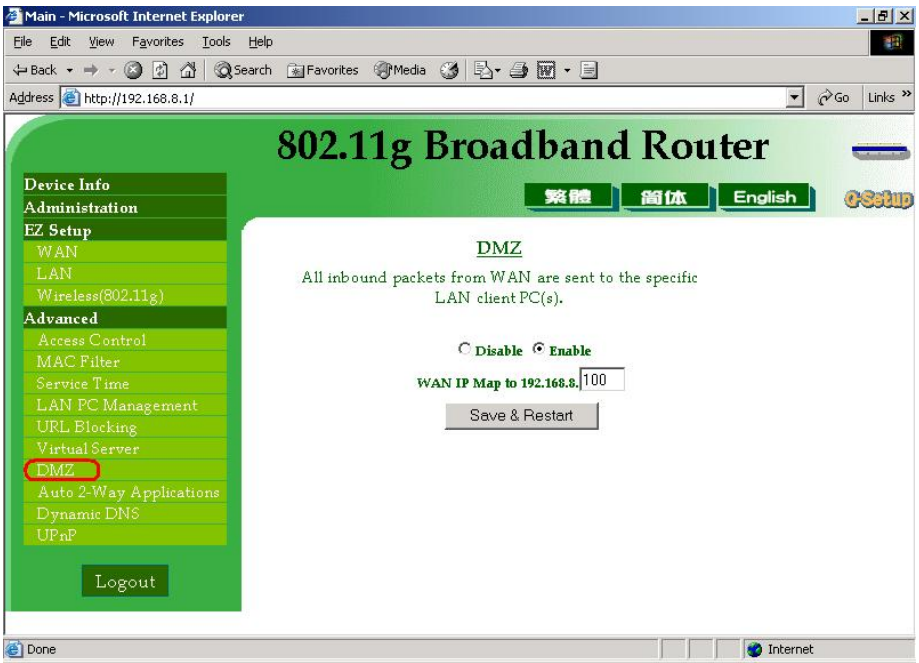


Figure 4.10 Single Demilitarized Zone

4.8 Multiple DMZ Host

In case WAN connection type is static and there are a range of IP addresses assigned to WAN interface instead of single IP only (please refer to Section 3.1), then the router allows up to 8 computers in LAN to become DMZ host (See Figure 4.11).

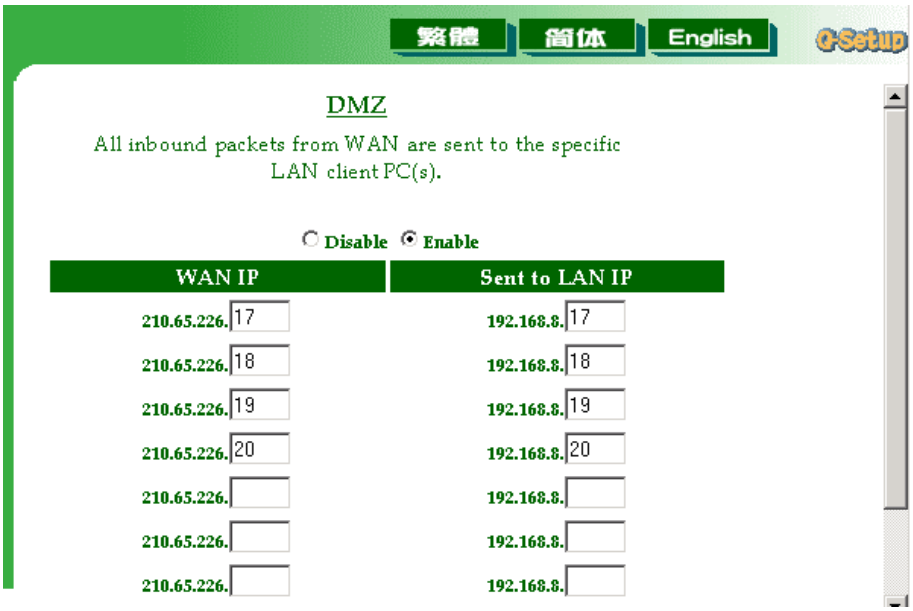


Figure 4.11 Multiple DMZ

In general, the mechanism of multiple DMZ hosts is based on the mapping relation between WAN IP and LAN IP (shown below). And these DMZ hosts will skip NAT port translation handling to gain unrestricted 2-way communication capability.

WAN IP1	ç	Broadband router	è LAN IP1 (DMZ host1)
WAN IP2	ç	Broadband router	è LAN IP2 (DMZ host2)
WAN IP3	ç	Broadband router	è LAN IP3 (DMZ host3)
……			
WAN IP8	ç	Broadband router	è LAN IP8 (DMZ host8)

For example, the ISP provides 210.65.226.0 ~ 7 IP range (subnet mask is 255.255.255.248), then subscriber could have 5 DMZ computers at most to access Internet simultaneously. The other computers are also able to access Internet via the router's NAT mechanism (Figure 4.12).

There are two types of connection configurations supported by the ISP. One is Bridging mode, the other is Routing mode. If a Bridging mode configuration is supported by your ISP, please enable **WAN is connected with Bridging Mode** option locating at the bottom of the DMZ

menu configuration. For a Routing mode supported ISP, just leave this option disable.

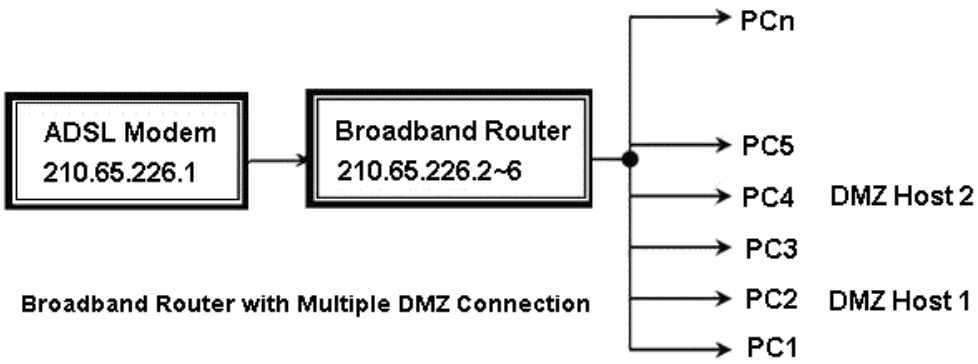


Figure 4.12 Broadband Router with Multiple DMZ Connection

4.9 Auto 2-Way Applications

From the above two sections (Virtual Server and DMZ), it can be concluded as follows:

1. Virtual Server can support those applications that are fully dependent on the incoming destination TCP/UDP ports regardless of the incoming destination IP address.
2. DMZ can support those applications which are dependent on the incoming destination IP address only, no matter which TCP/UDP port they used or no matter how many TCP/UDP ports they use simultaneously.

Although the router provides above two methods for compatibility improvement under the firewall protection, however there is some inconvenience for administrator to manage lots of PCs at home or in a SOHO environment. For example, in spite of Virtual Server or DMZ functions, administrator must know the specific LAN PC's IP address in advance. Then administrator could fill it into the WEB page for Virtual Server or DMZ. Nevertheless, if another LAN PC would like to use the same services, then administrator would perform the same setting again. It does not seem to be an automatic method.

For some special applications (like MS messenger, MS game zone, some VoIP device...), they always connect to an outside server with a fixed destination port, then the server would communicate with the application in LAN by using a predefined incoming port (or a specific range of incoming ports). In this case, the router can provide a fully automatic mechanism to support such kind of applications.

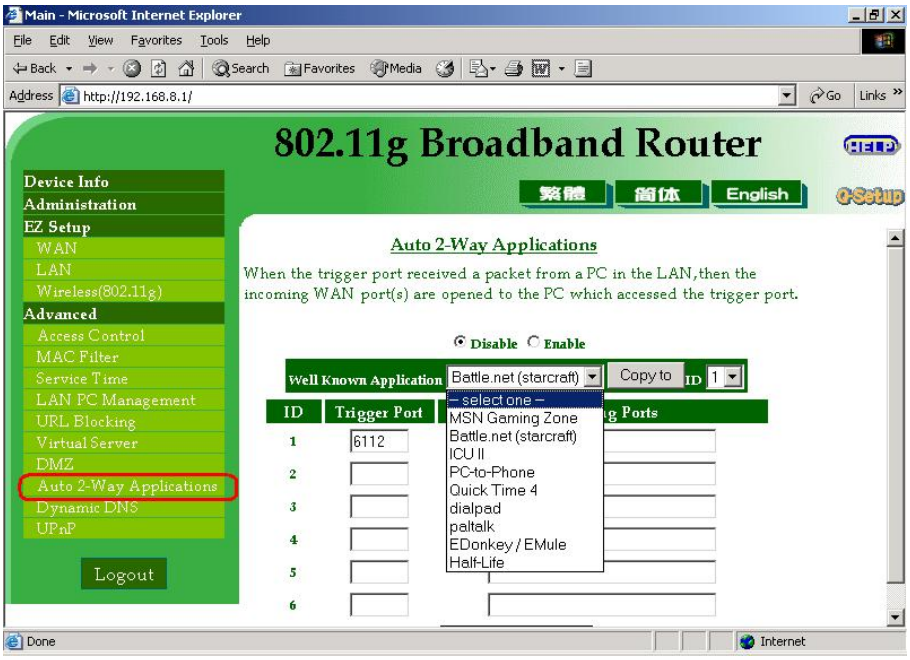


Figure 4.13 Auto 2-way Applications

Where:

Trigger Port: The application sends a packet out first to the trigger port.

Incoming Ports: All the packets incoming to the specified ports are allowed to pass the firewall.

There are several predefined well-known applications listed in the top of setting page. Select an application and click **Copy to** index ID.

Note:

For each trigger port, one and just only one LAN PC uses it at one time. Once a trigger port is occupied, the second or later LAN PC could not use that trigger port until the first LAN PC has released it. (Release means the first PC doesn't use that trigger port for more than 5~6 minutes).

4.10 Dynamic DNS

For most dial-up ADSL and Cable modem users, it is not easy to get a fixed WAN IP address when the router is connected with the Internet. (Whatever the router's WAN connection type is PPPoE, DHCP client or PPTP client, the WAN IP of the router is obtained from ISP side dynamically).

As a result, it is very difficult to host a Web server or FTP server like www.xxx.com or

ftp.yyy.net by using a dial-up ADSL or Cable modem. Fortunately, there are some non-profitable organizations (like www.DynDns.org…) or commercial dynamic DNS service provider (like www.dns2go.com or www.DynIP.com…) has proposed solutions to serve such applications.

All of these solutions are working in a similar way. They need a LAN PC (Intent access capable) to update their DNS server's record periodically to keep the WAN IP address up to date. Most of their differences are the update packet syntax or format, and how often the update event will occur – when dial up is successful or based on every N minutes interval.

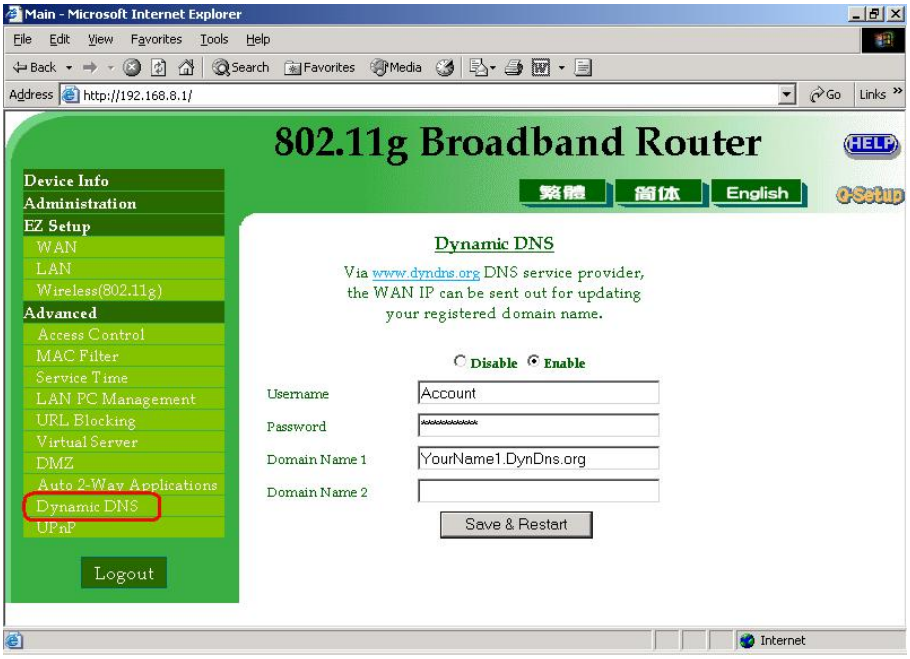


Figure 4.14 Dynamic DNS

The router has internally built in an update client function to meet www.DynDNS.org update spec. This means it could act as a dynamic DNS update client itself. Thus administrator doesn't need one more PC in LAN to install the update client program.

Certainly this function could be disabled (by default) when dynamic DNS is never used, or other dynamic DNS service provider is preferred.

Note:

1. After 5 minutes later, update event will occur whenever got a new WAN IP.
2. To enable this function, it is necessary to apply for a dynamic DNS account as your registered URL name.
3. Please visit www.DynDns.org for more detailed information.

4.11 UPnP (Universal Plug and Play)

"Universal Plug and Play" is designed to support zero-configuration and automatic discovery device categories from a wide range of vendors. With UPnP enabled, the Internet Gateway Device (IGD) could be discovered and detected by UPnP capable PCs. Thus IGD devices could be easily managed by Windows system. (It is supported by WIN-Me or WIN-XP only).

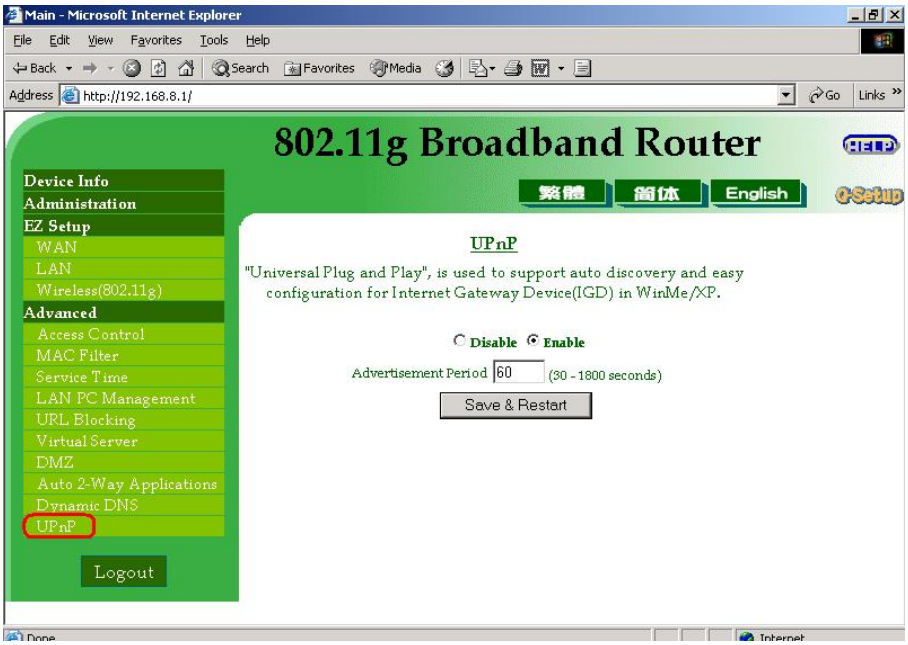


Figure 4.15 UpnP

Advertisement Period

The Advertisement Period is how often the router will broadcast its UPnP information. This value can range from 30 to 1800 seconds. Shorter durations will ensure that control points have current device status at the expense of additional network traffic. Longer durations may compromise the freshness of the device status but can significantly reduce network traffic.

5. Troubleshooting

5.1 Common Problems & Solutions

This section provides possible solutions to problems regarding the installation and operation of the router. Try to find answers here if there is any problem while you setup this device.

Check your device and settings step by step.

1. Failed to Connect to the router's LAN port

- The router is properly installed with appropriate LAN connections. (Please check ACT/Link LED)
- Set the router into factory default condition (by holding the reset button down for 5 seconds).
- Ensure that your PC and the router are on the same network segment. If you are not sure, initiate the DHCP function to let PC get IP address from the router automatically.
- Make sure that the IP address of your PC is 192.168.8.x.
- Check Subnet Mask value, it should be 255.255.255.0.

2. Failed to configure the router through web browser (by a client PC in LAN)

- Check the hardware connection of the router's LAN port.
- Check if the indicated ACT/Link LED on the front panel is working properly.
- In Windows9x/Me, run **winipcfg** (NT4/2000/XP, run **ipconfig**) to check the client side by clicking **Start/Run**. The PC should have:
  1) IP address: 192.168.8.xxx (xxx is from 17 to 128 by default).
  2) Submask: 255.255.255.0
  3) Default Gateway IP: 192.168.8.1

3. WAN can't obtain any IP address from a Cable or DSL modem in WAN.

- Ensure if the WAN LEDs are correctly illuminated (Refer to Appendix C for correct cabling).
- Power down your DSL or Cable modem for a few seconds. Turn it back on. After the modem goes through its self-test, check to see if you now have an WAN IP address.
- Your ISP may require MAC address, Host name, and Domain name. Check if they are correct.

4. "Time out error" message pops up when I enter a URL or IP address.

- Check if other PCs work. If they do, ensure that your workstations IP settings are correct (IP address, Subnet Mask, Default gateway and DNS...).
- If the PCs are configured correctly, but still not working, check the router. Ensure that it is connected and power on (If you cannot connect with it, check LAN and power connections).
- If the router is configured correctly, check your Internet connection to see if it is working well (by checking the WAN's IP address is valid or 0.0.0.0).

5. Lost or forgot Administrator password.

- Reset system setting (by holding **Reset** button down for 5 seconds) into factory default, this will restore administrator password to **admin**.
- Re-configure your router according to your previous setting.

6. Why my Notebook computer failed to connect with the router via wireless LAN card?

- Ensure if the router's wireless LED is correctly illuminated.
- Check your computer's wireless LAN setting (like SSID, channel number) is the same as the router.
- Check WEP-64 or WEP-128 is enabled or not. If it is on, the key must be the same.
- Most wireless LAN cards provide a monitor/diagnosis utility, please use the utility in your computer to check the wireless signal strength and link quality. The more closer to the router, the better signal quality.

5.2 Frequently Asked Questions

1. Where is the router installed on the network?

Typically, it is installed between Cable/DSL modem and LAN. Plug the router's WAN port into Cable/DSL modem's Ethernet port. (Refer to Appendix-C for connect cabling.)

2. Does the WAN connection of the router support 100Mb Ethernet?

Yes, it does support 10/100Mb Ethernet on its WAN port. Since the router's WAN is an auto-sensing 10/100 port, it is also compatible with 10Mb-only WAN devices.

3. What is NAT (Network Address Translation) and what is it used for?

NAT translates multiple private IP addresses in LAN into one public address (in WAN) that is sent out to the Internet. NAT has 2 functions:

- It adds a level security since the IP address of a PC connected to the private LAN is never transmitted on the Internet.
- NAT allows the router to be used with low cost Internet accounts, such as DSL or cable modems, which only one IP address is provided by ISP. Users can have many private addresses behind this single address provided by ISP.

4. If the router is totally failed in the installation, what can I do for it?

Reset the router by holding down the **Reset** button for at least 5 seconds and reset your cable or DSL modem by powering the unit off and then on.

5. What can I do if l lost connection with the router when I change the LAN subnet from 192.168.8.1 to 192.168.1.1 (or like others)?

This problem is often caused by that your LAN client PC is no longer the same subnet address as the router. The solution is just to release your LAN client PC's IP address then renew it (most likely, IP address becomes 192.168.1.x).

6. With which type of firewall is the router equipped?

It uses NAT and TCP/IP stateful packet inspections.

7. What can I do when I am not able to get the web configuration screen for this router?

You may have to remove proxy settings on your Internet browsers or remove dial-up settings on your browser (especially if you use PPPoE WAN connection).

8. What is DMZ (Demilitarized zone)?

DMZ allows one IP address (computer) to be exposed to the Internet. Some applications require multiple TCP/IP ports to be opened. It is recommended that you set your computer with a static IP if you want to use DMZ.

9. Does the router pass PPTP or actively route PPTP sessions?

Yes, this router allows PPTP packets to pass through.

10. Is the router cross-platform compatible?

Yes, any platform that supports Ethernet and TCP/IP is compatible with the router (like Windows 9x/Me/NT4/2000/XP, Linux, iMac, Unix…).

11. Can I use my own public IPs and Domain or I have to use the IPs provided by this router?

You can customize your own IPs through configuration of this router.

12. What are the advanced features of the router?

The advanced features of the router include Access Control, URL Blocking, Virtual Server, DMZ, Auto 2way application and DDNS.

13. Does the router support ALG (Application Layer Gateway) functions?

Yes, the following ALG functions are supported:

FTP	: passive mode and port command mode.
Conferencing	: MS NetMeeting, H.323 pass though.
Instant Messenger	: MS MSN messenger, Yahoo messenger, ICQ, AOL.
L2-VPN	: PPTP client mode, PPTP pass through
IP-VPN	: IPSec (ESP) pass through
Gaming	: AOE, CS, Star-Craft…

Appendix A Well-known TCP/IP Ports

Any application or process that uses TCP for its transport is assigned a unique identification number called a TCP port. TCP ports specify the path of communications between client and server applications. These ports are numbered beginning with zero. Port numbers for client applications are dynamically assigned by the operating system when there is a request for service. Port numbers for server applications are pre-assigned by the Internet Assigned Numbers Authority (IANA) and are not changed. Following is a short list of some well-known port numbers.

Table A-1 Well-known TCP Ports

Port No.	Name (TCP)	Description
20	FTP-DATA	FTP (data)
21	FTP	FTP (command)
23	TELNET	Terminal Connection
25	SMTP	SMTP
53	DOMAIN Name	Domain Name Server
79	FINGER	Finger
80	HTTP	Web
110	POP3	POP3
113	AUTH	Authentication Service
139	NETBIOS-SSN	NETBIOS Session Service
1723	PPTP	Point to Point Tunneling Protocol

Appendix B Illustrated Typical Application

B-1 Home User Application

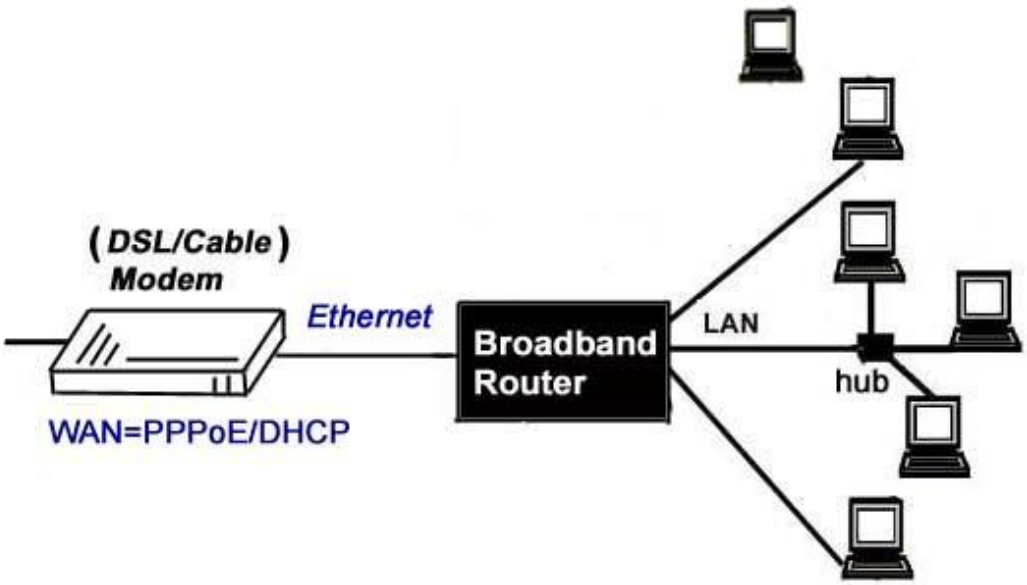


Figure B-1 Home User Application - DSL/Cable Modem

B-2 SOHO Environment Application

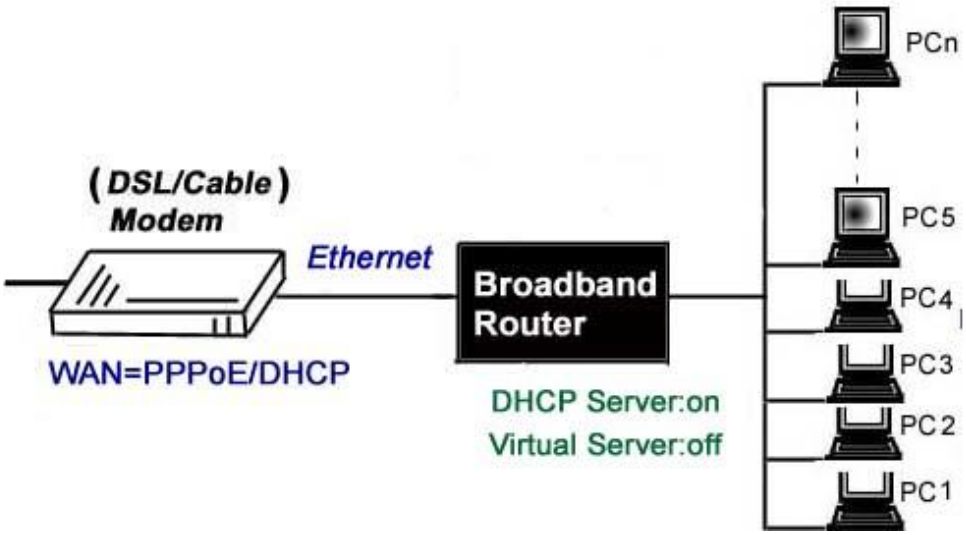


Figure B-2 SOHO Environment Application – Simple IP Sharing

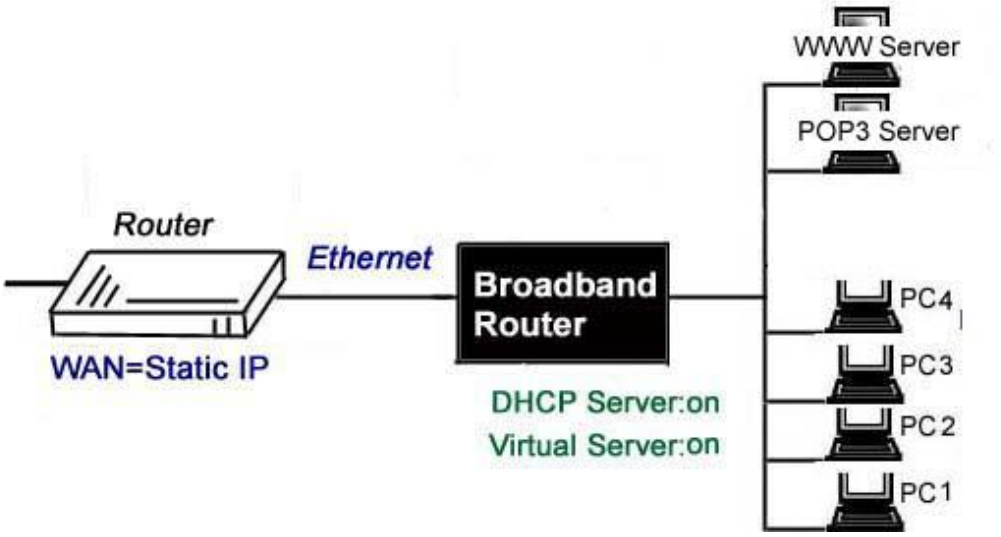


Figure B-3 SOHO Environment Application - DHCP Server in the router

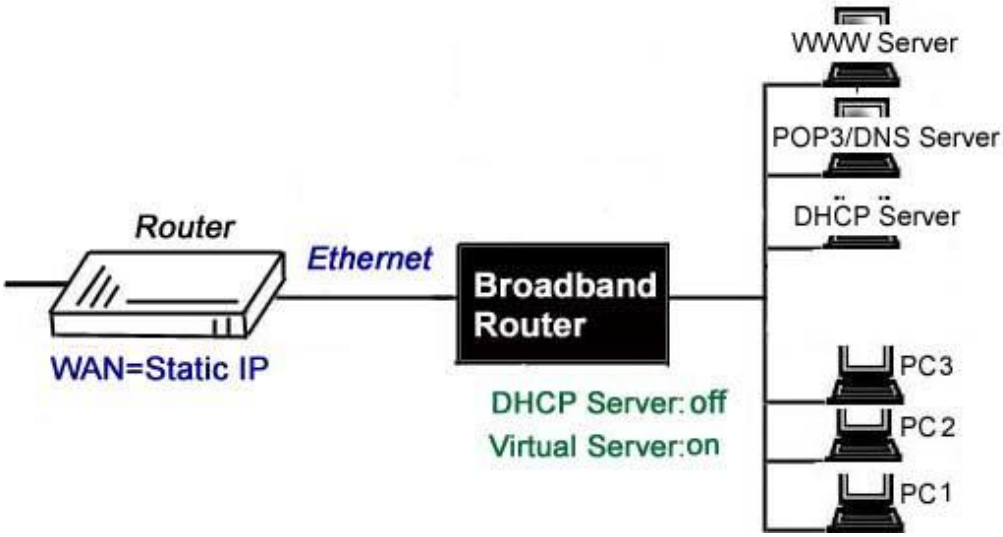


Figure B-4 SOHO Environment Application – DHCP Server in LAN

Appendix C Cabling and Pin Assignment

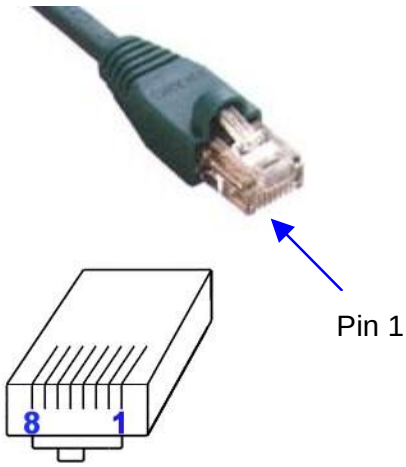
There are different grades, or categories, of twisted-pair cabling. Category 5 is the most reliable and is highly recommended. Category 3 is a good second choice. Straight-through cables are used for connecting computers' NIC card to a hub. Crossover cables are used for connecting a hub to another hub (the router provides a built-in uplink/normal switch, uplink mode is crossed internally, which allows you to link or connect hubs together with a straight-through cable instead).

RJ-45 pin assignment

There are 8 thin, color-coded wires inside, run from one end of the cable to the other. All 8 wires are used.

Table C-1 RJ-45 Connector

RJ-45 Color Chart	
Wire 1	White with an Orange stripe
Wire 2	Orange
Wire 3	White with a Green Stripe
Wire 4	Blue
Wire 5	White with a Blue Stripe
Wire 6	Green
Wire 7	White with a Brown Stripe
Wire 8	Brown



To determine which wire is wire number 1, hold the cable so that the end of the plastic RJ-45 tip (the part that goes into a wall jack first) is facing away from you. Face the clip down so that the copper side faces up (the springy clip will now be parallel to the floor), when looking down on the copper side, wire 1 is on the far left.

Connection between NIC card and Hub

A **straight-through** cable, wire 1,2,3,and 6 at one end of the cable are also wires 1,2,3, and 6 at the other end. The straight-through cable is used in connecting the NIC card and the hub. See Table C-2.

Table C-2 Pin Assignment of Straight Through Cable

Straight Through Cabling		
Wire		Becomes
1	⇨	1
2	⇨	2
3	⇨	3
6	⇨	6

Connection between Hub and Hub

In a **crossover** cable, the orders of the wires change from one end to the other. Wire 1 becomes 3, and 2 becomes 6. The crossover cable is used in connecting hubs directly. See Table C-3.

Table C-3 Pin Assignment of Crossover Cable

Crossover Cabling		
Wire		Becomes
1	⇨	3
2	⇨	6
3	⇨	1
6	⇨	2

Appendix D Configure IP manually

1. Select **IP Address** tab, and then choose **Specify an IP Address** (see Figure D-1). Type in your customized IP address (the default IP address of this product is 192.168.8.1. So you just can type in one IP Address like 192.168.8.xxx. Where xxx can be numbers from 2 to 254). Set the Subnet Mask as 255.255.255.0.

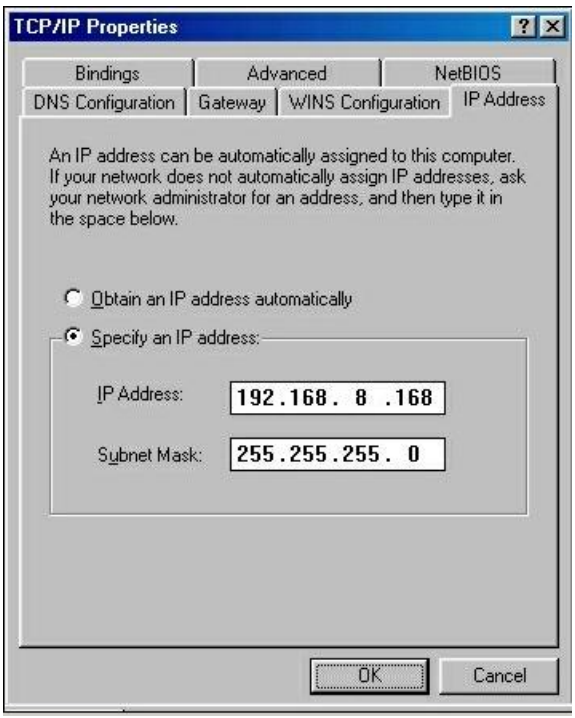


Figure D-1 Configure IP Manually

2. Click **Gateway** tab, and add IP address of the router (the default IP Address is 192.168.8.1). See Figure D-2.

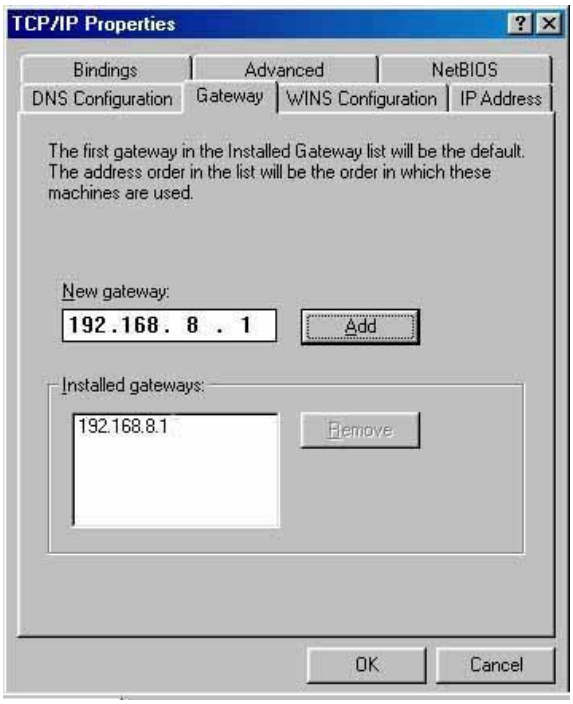


Figure D-2 Add Gateway Address

3. Change to **DNS Configuration** tab; enable DNS and add DNS values provided by your ISP into **DNS Server Search Order**. See Figure D-3.

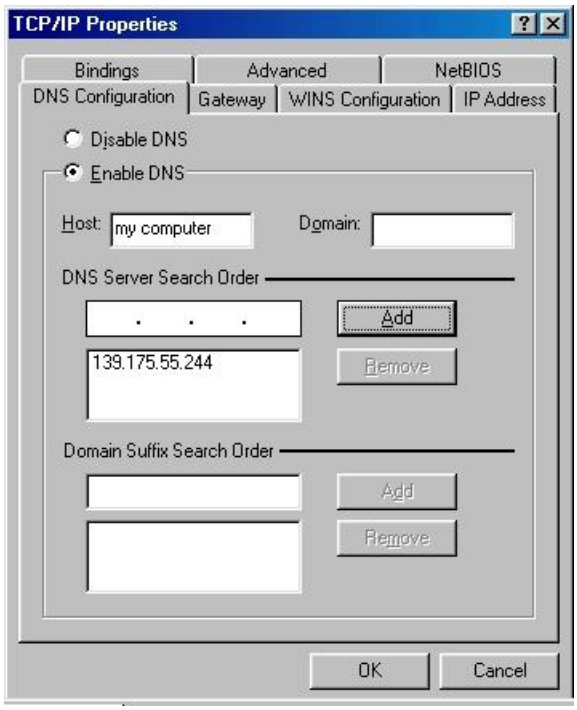


Figure D-3 Enable DNS and Add DNS Values

4. Click **OK** to finish.

Appendix E Technical Information

Operational

WAN I/F	: One RJ-45 port, 10/100Base-T, Auto-MDI/MDIX
WAN cabling	: UTP category 5 (10/100 Mbps)
LAN I/F	: Four RJ-45 ports, 10/100Base-T, Auto-MDI/MDIX
LAN cabling	: UTP category 5 (10/100 Mbps)
Wireless LAN	: IEEE 802.11b/g, support 1/2/5.5/6/9/11/12/18/24/36/48/54 Mbps
LED indication	: Power, Ready, WLAN, WAN, LAN
Reset button	: Restore factory default

Environmental

Power Input	: External, DC 5V/2A
Dimensions	: 8.7” x 5.2” x 1.5” (220 x 132 x 38 mm)
Unit Weight	: 15.5 oz. (440 grams)
Certification	: FCC class B, CE mark
Operating Temperature	: 0°C to 40°C
Storage Temperature	: -20°C to 70°C
Operating Humidity	: 0% to 90%, non-condensing